VA Office of Information and Technology

Office of Enterprise Architecture Management

Systems Integration and Development Service (SIDS)

Configuration Management Plan

V1.0

April 17, 2006

VA Office of Information and Technology
Enterprise Architecture Management
Systems Integration and Development Service

Letter of Promulgation

This Configuration Management Plan (CMP) for the System Integration and Development Service (SIDS) of the Office of Enterprise Architecture Management (OEAM) in the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), establishes a structured approach for managing changes during the evolution of SIDS management and products produced by the SIDS and during the subsequent operations and maintenance of those products. This plan:

a. Helps ensure compliance with SIDS CM policy and OEAM provisions of the Information Technology Management Reform Act (Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3))),
b. Facilitates the alignment of the organization with the Carnegie-Mellon University Software Engineering Institute Capability Maturity Model Integration (CMU/SEI CMMI),
c. Defines the SIDS approach to CM,
d. Allocates SIDS CM roles and responsibilities,
e. Provides the SIDS activities to be performed for implementing a service-wide, integrated CM system for SIDS assets and products,
f. Clarifies and enhances current SIDS CM practices, and
g. Directs their application across the SIDS organization.

This SIDS CM Plan is intended to work within the framework of the SIDS organization structure and within constraints of the duties, responsibilities, and authorities granted to the SIDS organization by higher authority.

As the Director, Systems Integration and Development Services (SIDS), I do hereby formally promulgate this CM Plan and direct its execution and use across SIDS.

___(Signature obtained and on file)____ *____April 17, 2006____*
Frances G. Parker, Director (Acting) (Date)
Systems Integration and Development Services
Office of Enterprise Architecture Management
VA Office of Information and Technology

Record of Changes

Version #	CCP #	Description	Date Entered	Entered by:
1.0	N/A	Initial Issue	4/17/06	bgl

Table of Contents

This Page Intentionally Blank

1. INTRODUCTION

This document is the Configuration Management Plan (CMP) for the Systems Integration and Development Service (SIDS). SIDS, an organization within the Office of Enterprise Architecture Management (EAM) of the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T), is the organization responsible for engineering, development, and integration of assigned information technology (IT) assets.

Configuration Management (CM) is a formal engineering discipline that provides stability to the evolution of products and enhances product integrity, quality, and reliability in a visible and traceable manner. CM is the means by which the enterprise system and subsystems are identified, managed, monitored, and confirmed. An effective CM effort throughout the OI&T enterprise is an absolute necessity for the delivery and maintenance of an error-free and reliable automated system on time and within budget.

1.1. PURPOSE

The purposes of this SIDS CMP are to:

1. Provide direction and guidance for executing the SIDS CM Policy,
2. Establish the SIDS CM organization structure, roles, and responsibilities,
3. Describe and define CM activities necessary to establish and maintain the integrity of SIDS work products and assets,
4. Provide governance and guidance for CM as an enterprise effort across the SIDS,
5. Promote SIDS management commitment to oversight and planning of VA IT assets assigned to SIDS,
6. Address CM training for SIDS CM personnel and others with CM responsibilities,
7. Facilitate continuous process improvement across all SIDS program, business, and information technology communities, and
8. Contribute to the successful achievement of other SIDS and OI&T enterprise architecture goals.

1.2. SCOPE

This CMP applies to all organizational levels, products, and IT assets of SIDS including but not limited to offices, projects, and activities that are the responsibility and under the authority of the Director, SIDS. Any deviation from this plan is authorized only upon submittal and Director, SIDS, approval of a documented Request for Waiver (RFW) through the defined RFW procedure. (Refer to Request for Waiver (RFW) Procedure – TBD.)

SIDS IT assets include all management, software, hardware, technology infrastructure, and related documentation used in satisfying SIDS mission including, but not limited to, SIDS management publications, computer programs, source code listings, Integrated Development Environment (IDE) tools, control tools, processes, associated documentation, networks, and associated drawings, blueprints, and schematics.

This plan also applies to any item resulting from SIDS mission changes and designated for formal configuration change management by SIDS or higher authority throughout the life of SIDS mission.

1.3. AUTHORITY

This CMP is issued under the authority of and takes effect immediately upon approval of the Director, SIDS. Upon approval, this document is a configuration item and may be modified or cancelled only through the Configuration Change Proposal (CCP) process as described in the "Configuration Change Management" section below. The Director will ensure that this CMP is reviewed at least annually for accuracy, currency, and completeness.

1.4. MODIFICATIONS AND CANCELLATION

There are no documents replaced or superseded by this plan. Any changes to this plan or any portion of it shall be introduced according to instructions in the Configuration Change Management section of this plan.

1.5. PLAN STRUCTURE AND CONTENT

This document is arranged and presents information as indicated below:

Section 1 – Introduction
Provides information about this plan – why it has been written, what it governs, who authorized it, what it replaces, and a description of its structure and content.

Section 2 – Standards
Presents special terminology and lists reference materials.

Section 3 - Project Environment
Describes the "corporate" organizational structure, the operational background in which this CM effort is to be performed, and the assumptions under which this CM Plan is implemented.

Section 4 – SIDS Configuration Management Organization
Describes SIDS CM structure for executing this plan and sets the roles and responsibilities required and assigned.

Section 5 – CM Activities and Operations
Presents the activities and operations called forth in executing this plan.

2. STANDARDS

2.1. TERMS AND ABBREVIATIONS

Refer to Appendix A for the terms and abbreviations used in this plan.

2.2. REFERENCES

1. Clinger-Cohen Act of 1996 (Public Law 104-106).
2. Department of Veterans Affairs Directive 6000.
3. Electronic Industries Alliance (EIA)/Government Electronic and Information Technology Association (GEIA) Standard-649-A, National Consensus Standard for Configuration Management, April 2004.
4. Carnegie-Mellon University/Software Engineering Institute (CMU/SEI), Capability Maturity Model Integration for Systems Engineering/Software/Integrated Products and Processes Development/Supplier Sources, March 2002.
5. Electronic Industries Alliance (EIA) Standard 836, Configuration Management Data Exchange and Interoperability, June 2002.

3. PROJECT ENVIRONMENT

3.1. BACKGROUND

SIDS is committed to functioning as a unified, single-source organization for engineering, development, and integration of IT assets assigned by higher VA authority and in support of the "OneVA" concept. OneVA is an evolutionary, high-performance, information technology architecture aligned with the program and business goals to enable VA enterprise-wide integration of functions, processes, and data.

Successful establishment of the envisioned OneVA capability requires improved business processes, more consistent information, greater accessibility, and better efficiency for a more customer-centric approach. These improvements can be realized through improved IT resource utilization achieved by:

- Identification and elimination of redundancies,
- Integration of resources, and
- Coordination of additions to and modifications of IT resources.

3.2. ORGANIZATIONAL ENVIRONMENT

OI&T, headed by the Chief Information Officer (CIO), is responsible for all IT assets of the VA. Those assets include not only the hardware, firmware, software, and "technical" documentation belonging to the various Administrations, Services, Divisions, and other offices within the VA organization, but also include the documents, designs, plans, procedures and processes whereby the assets are managed. (Figure 1 on page 6 illustrates the VA organizational structure and shows SIDS within it.)

The Department of Veterans Affairs consists of:

Veterans Hospital Administration,
Veterans Benefits Administration,
National Cemetery Administration and
Other offices to support the Administrations.

The Administrations and other VA offices provide business needs and requirements to the OI&T through the Enterprise Oversight Committee (EOC). The EOC passes the needs and requirements through OI&T processes to SIDS, or other appropriate OI&T staff elements, for solution and fulfillment.

In support of SIDS organization, the SIDS CM team assists the Director, SIDS, with oversight for planning, tailoring, and implementation of CM Plans (CMP) and efforts relevant to the delivery of the solutions. (Figure 2 on page 7 illustrates the SIDS organizational structure.)
((Section 3.2 continued on Page 8))

QUESTION: EOC or EIB and what is

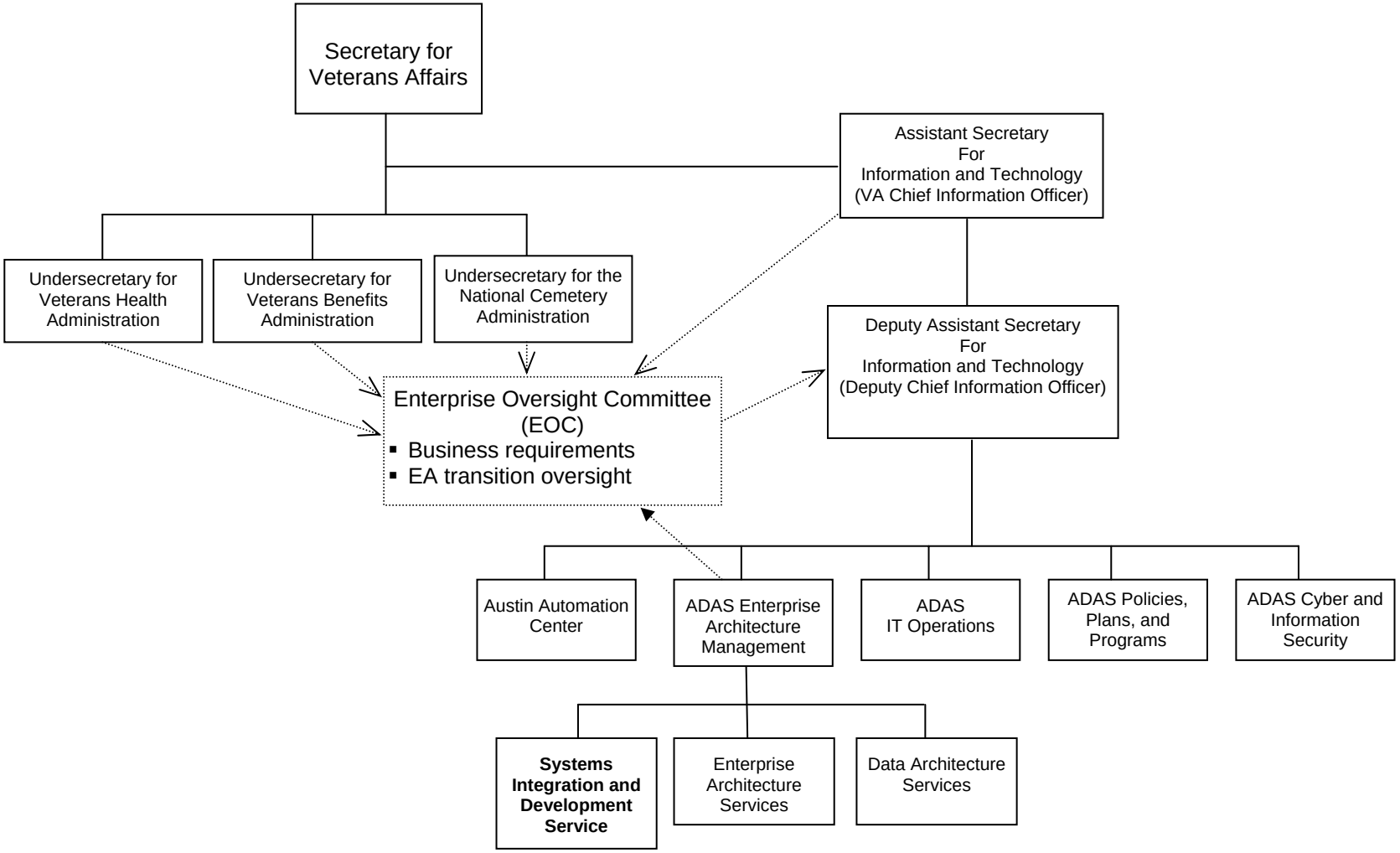
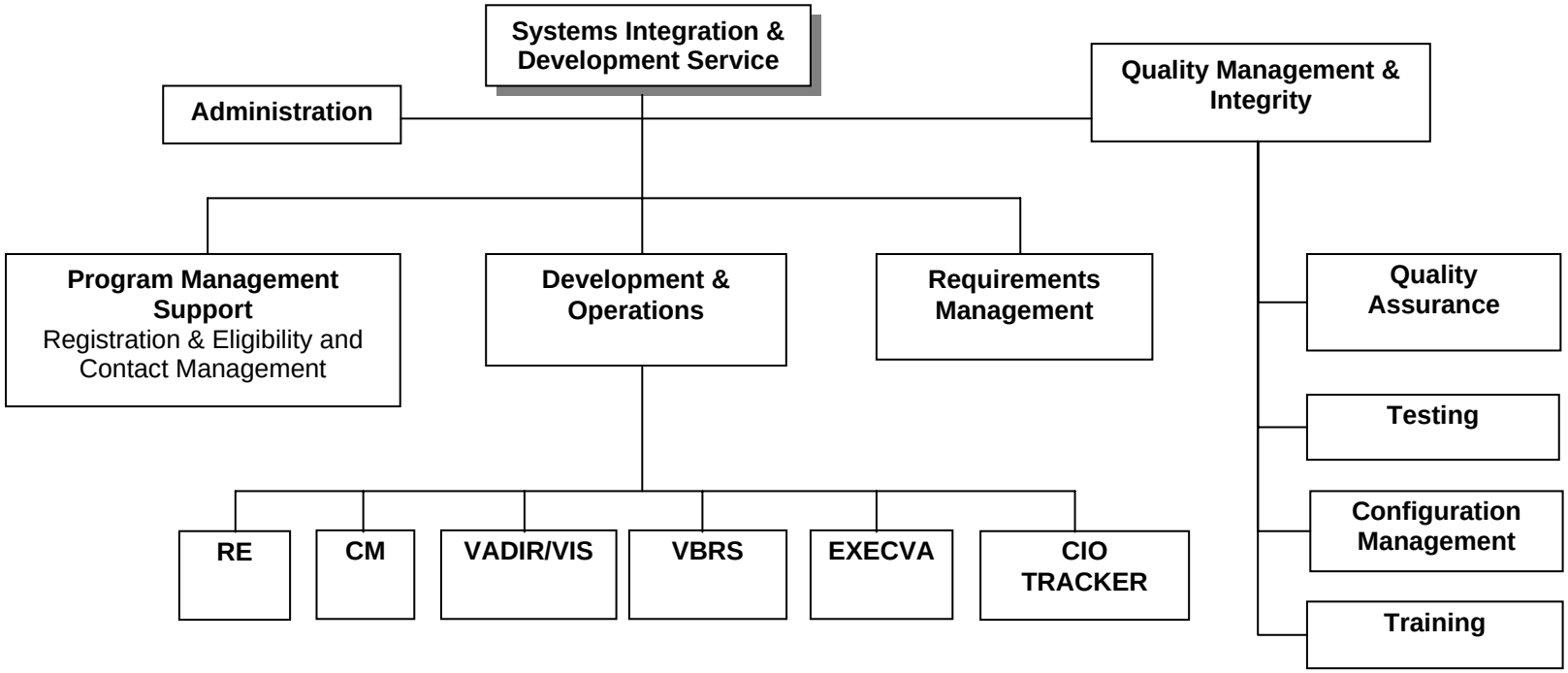


Figure 1 - VA Business Organizational Structure



NOTES:
1. A single Gov't person may exercise oversight for more than one project or oversight for more than one function within a project.
2. Other Gov't oversight functions may include, but are not limited to: Measurement & Analysis, Project Tracking, Risk Management, etc. These functions provide direct Government oversight over the projects.
3. The Management Oversight entities develop standards and processes, provide guidance and expertise to their respective Government counterparts on the projects, and independently assess and measure project compliance with established standards and procedures.

Figure 2 - SIDS Organizational Structure

Additional SIDS CM team responsibilities include, but are not limited to:

1. Implement and maintain SIDS CMP,
2. Develop and maintain approved tools to support CM plans and procedures (tools such as checklists, sign-off sheets, training materials, inventories, automated applications, etc.),
3. Ensure compliance with the SIDS CMP,
4. Provide CM training and orientation as necessary to CM participants,
5. Assist in CI selection,
6. Assign CI Identifiers to configuration items and components,
7. Ensure the security and integrity of CM-controlled baseline files (hardware, software, documentation, COTS, Networks, libraries, publications),
8. Ensure compliance with Configuration Change Management (CCM) requirements,
9. Coordinate change management tasks and activities,
10. Assist with change incorporation when necessary,
11. Assist with change implementation when necessary,
12. Perform and support review and audit activities,
13. Provide status accounting oversight,
14. Maintain records, databases, and libraries (repositories),
15. Help define appropriate CM reports,
16. Generate CM reports.

3.3. TECHNICAL ENVIRONMENT

The network operating systems of the VA are primarily Microsoft Windows Server 2000 or later. The majority of databases run on various Oracle and Structured Query Language (SQL) systems. SIDS desktops are Microsoft Windows XP.

All SIDS management documentation is developed in the Microsoft Office suite of applications (or Director-designated equivalents) and prepared in accordance with SIDS documentation standards and guidelines. All other information technology products and artifacts will be developed, produced, and tested in accordance with the Department of Veterans Affairs Technical Reference Model and Standards Profile. Waivers and deviations from these requirements must be requested by a formal written Request for Waiver/Deviation. Waivers and deviations may be implemented only upon written approval by or at the written direction of the Director, SIDS, or higher authority. (Refer to Section 4.4 for CM-Specific Information.)

SIDS recognizes that special workstation setups are required to satisfy special development and maintenance needs. The Director, SIDS, has the right to place such special workstation setups under formal configuration control (usually due to significant costs for licensing, extra-large monitor screen requirements, computer capacity, etc., or by direction of higher authority).

4. SIDS CONFIGURATION MANAGEMENT ENVIRONMENT

The SIDS CM structure is a hierarchy of Configuration Change Management Boards (CCMB) that controls the configurations of assets under the responsibility of SIDS. The tiered CCMB framework provides a systematic methodology to:

- Establish SIDS hardware, firmware, software, and document baselines,
- Propose, justify, evaluate, coordinate, and approve or disapprove changes,
- Implement all approved changes to baselines,
- Identify impacts across organizational lines (i.e., organizational interfaces), and
- Facilitate decision-making at the lowest practical level in the SIDS organization. "Lowest practical level" in this context is that level:

    1) Where the necessary knowledge for decision making is available,
    2) Where all sides of affected configuration interfaces are represented, and
    3) To which the authority to make the decision has been delegated.

Allowing decision-making at the lowest practical level requires a scheme of "checks and balances" to promote an integrated enterprise system. Sections 4.1 through 4.3 below present the tiered SIDS CM structure and the schema by which checks and balances are implemented.

4.1. SIDS CM ORGANIZATION STRUCTURE

The SIDS CM structure is based upon levels of appropriately allocated change control authorities to facilitate efficient and effective satisfaction of product requirements and change management responsibilities. These levels of authority permit decisions to be made at the lowest practicable level while providing a system of checks and balances to ensure that higher authority is not infringed upon and that interface decisions are properly authorized.

4.1.1. Explanation of CM Levels

The CM levels within the VA OI&T are identified to facilitate allocation of control responsibilities to the OI&T Office and to place the authority of the SIDS internal CCMB structure within context. These levels do not apply to the internal levels of contractors. The SIDS CCMB structure and authority levels generally follow the OI&T organizational structure and are identified as follows:

Level A. Reserved for OI&T Executive level – Items that result in changes to OI&T controlled milestones, publications (and other documents), or significant changes to budget requests.

Level B – Enterprise Architecture Management (EAM) – Items not reserved to the OI&T Executive level or higher authority and:

a) Those requiring approval and signature by the Associate Deputy Assistant Director (ADAS), EAM;

b) EAM organization documents; functional and performance requirements of Level C organizations;
c) Level C management documents and publications (e.g., Charters, Plans and organization structures);
d) EAM inter-Service and inter-Division Interface Control Documents;
e) Technical and management items having an impact across two or more Services or Divisions (or sub-elements within two or more Branches); and
f) Other such items as the ADAS, EAM, may direct.

Level C – Systems Development and Integration Services (SIDS) – Items not reserved to the ADAS EAM or higher authority and:

a) Those requiring approval and signature by the Director, SIDS;
b) SIDS organization documents;
c) Functional and performance requirements of Level D organizations;
d) Level D management documents and publications (e.g., Branch Charters, Plans and organization structures);
e) SIDS inter-Branch Interface Control Documents; technical and management items having an impact across two or more Branches (or sub-elements within two or more Branches); and
f) Other such items as the Director, SIDS, may direct.

Level D –SIDS Direct-Report sub-organizations (To be used only if/when SIDS sub-organizations are established) – Items not reserved to the Director, SIDS, or higher authority and:

a) Those requiring approval and signature by the relevant Branch Head;
b) Branch organization documents;
c) Functional and performance requirements of Level E organizations;
d) Level E management documents and publications (e.g., Project or Management Group Charters, Plans and organization structures);
e) Inter-Project (or inter-Management Group/inter-product) Interface Control Documents;
f) Other technical and management items having an impact across two or more intra-Branch Projects or Management Groups (Project-level interfaces only); and
g) Detailed management requirements of Projects and Management Groups.

Level E – Projects and Management Groups – Items not reserved to higher authority and:

a) Those requiring approval and signature by the relevant Project Manager or Management Group Manager;
b) Project and Management Group organization documents; functional and performance requirements of Level F sub-elements;
c) Level F management documents and publications;
d) Intra-Project or intra-Group module/sub-element Interface Control Documents;
e) Other technical and management items having an impact across two or more modules within a Project or Management Group (module interfaces only); and
f) Detailed management requirements of Project/Group sub-elements.

Level F – Project or Management Group sub-elements (will usually be established only for very large or complex Projects or Management Groups and may be established for projects only during those periods or phases prior to deployment). The Level E Project Manager or Management Group Manager must provide written delegation, with justification, of control and authority below Level E. – Level E includes items not reserved to nor requiring approval or signature by higher authority and for which control and authority have been specifically delegated by the relevant Level D (SIDS sub-organization) Manager or the Director, SIDS.

The technical content of a change, not the level of the organization responsible for maintaining the baseline document, is the determining factor for the level at which a change may be approved. Interface responsibilities assigned to a level may not be delegated to a lower level. Figure 3 on the next page represents the hierarchical concept of SIDS CM and CCMB structure.

A "checks and balances" schema promotes an integrated system by ensuring that all affected EAM, and SIDS offices and staff are appropriately informed and afforded opportunity for input to the decision making process. Each CCMB within the SIDS organization should have representation from offices outside the SIDS organization (such as security, network services, legal, etc.) or specify them as addressees for new CCPs and meeting minutes to afford them the opportunity for analysis and inputs to the decision-making process.

4.2. SIDS CM ROLES AND RESPONSIBILITIES

CM is role-centric activity. A role is a unit of defined responsibilities that may be assigned to an individual, to several individuals, or to an organized group. Roles are independent of pay grade, job title, office name, etc.; however, roles may be assumed or assigned according to those characteristics. A single person may have multiple roles (such as senior executive, meeting chairperson, meeting facilitator), multiple users can have the same role (such as voting staff members), or groups, acting as unified entities, may have roles (such as a research committee or a control board).

4.2.1. Director, Systems Integration and Development Service

The Director, SIDS, has the responsibility and authority for acceptance of all IT work products and artifacts produced and approved within SIDS through the SIDS CCMB and for delivery to EAM and the VA Chief Enterprise Architect/CIO or directly to another recipient if so designated by higher authority. Within the SIDS, the Director, with EAM approval, may delegate acceptance authority to an appropriate deputy.

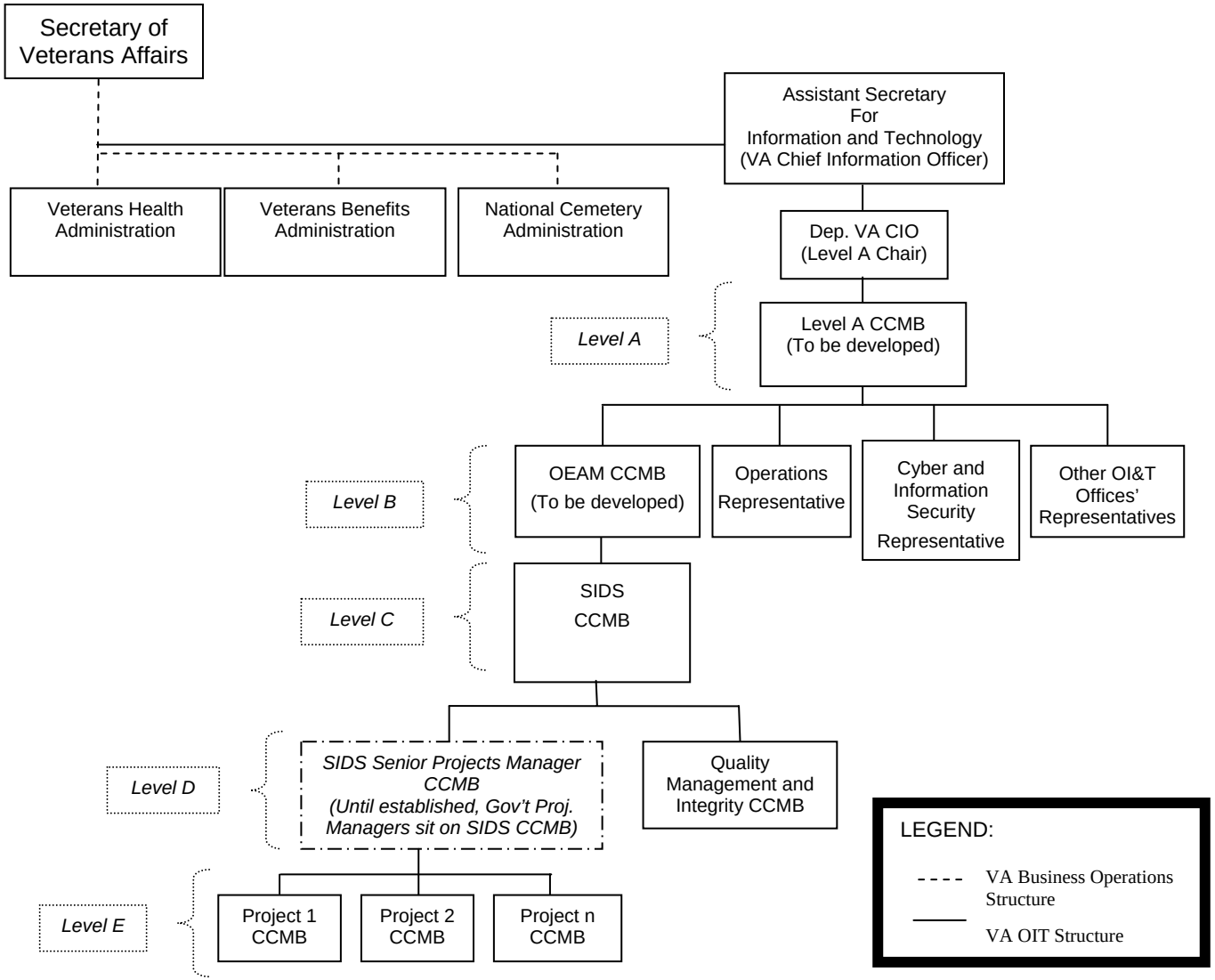


Figure 3 –Tiered CCMB Structure

The CM responsibilities of the Director, SIDS, include:

- Establish and enforce SIDS CM Process.
- Establish SIDS CM Planning Process.
- Ensure the identification of all common data, services, integration points and interdependencies among projects within the IT portfolio.
- Ensure the proper synchronization of projects to accommodate those interdependencies across the overall IT portfolio.
- Identify any integration or synchronization issues between SIDS and other VA organizations to the VA Chief Enterprise Architect.

The Director, SIDS, represents all SIDS entities and sub-organizations to the EAM. When a formal CCMB is established at the OI&T EAM level, the Director, SIDS, (or the properly designated Chair of SIDS CCMB) will represent SIDS on that board and serve as the interface conduit between all SIDS CM entities and the other EAM CM organizations.

4.2.2. SIDS Configuration Change Management Board

The Director, SIDS, established the SIDS CM effort to facilitate proactive management control over the products produced by the Service. In addition to creating a disciplined methodology for controlling SIDS management documentation, the SIDS CM effort is responsible for establishing the framework for an integrated SIDS CM system and for CM oversight and guidance at all internal levels and for all IT efforts within SIDS.

The SIDS Configuration Change Management Board (SIDS CCMB) Charter delineates the specific responsibility, authority and constraints of the SIDS CCMB and is to be referenced as the authoritative source. The Director, SIDS, established the SIDS CCMB:

- To exercise high-level, broad scoped management and control over the development and operation of SIDS IT assets and SIDS management architecture as a whole,
- To coordinate and manage IT interfaces between or among SIDS, SIDS staff elements, and other internal sub-organizations,
- To ensure that products developed by SIDS comply with applicable U.S. Government, Department, customer, and security requirements, and
- To preclude changes to SIDS-developed systems without proper review and approval.

The SIDS CCMB is comprised of the CCMB Chair, the secretariat, voting members, advisory members, and subject matter experts (Refer to Figure 4, next page). The Director, SIDS, appoints the SIDS CCMB Chair, who reports SIDS CCMB recommendations and findings to the Director for IT planning purposes. The Director may serve in the role of CCMB Chair or may assign a SIDS senior staff member to CCMB Chair duties if it is desirable to separate the duties of the Director, SIDS, and SIDS CCMB Chair (usually for purposes of objectivity). The Chair, Voting Members and Advisory Members and alternates of the SIDS CCMB must be employees of the Department of Veterans Affairs.

Participation of all voting members is required at each CCMB meeting. The SIDS CCMB reviews and votes recommendations to the Director, SIDS, to approve or disapprove proposed

baseline changes. Recommendations are made on the majority vote of all voting members (dissenting opinions/substantive positions are recorded). The Chair votes only to break a tie. Any Voting Member who disagrees with the majority vote shall file a minority opinion for conflict resolution by the Director, SIDS (who may defer to the ADAS, EAM). Any Advisory Member may file a minority report on a SIDS CCMB recommendation and should do so if the recommendation negatively impacts that member's area of responsibility.

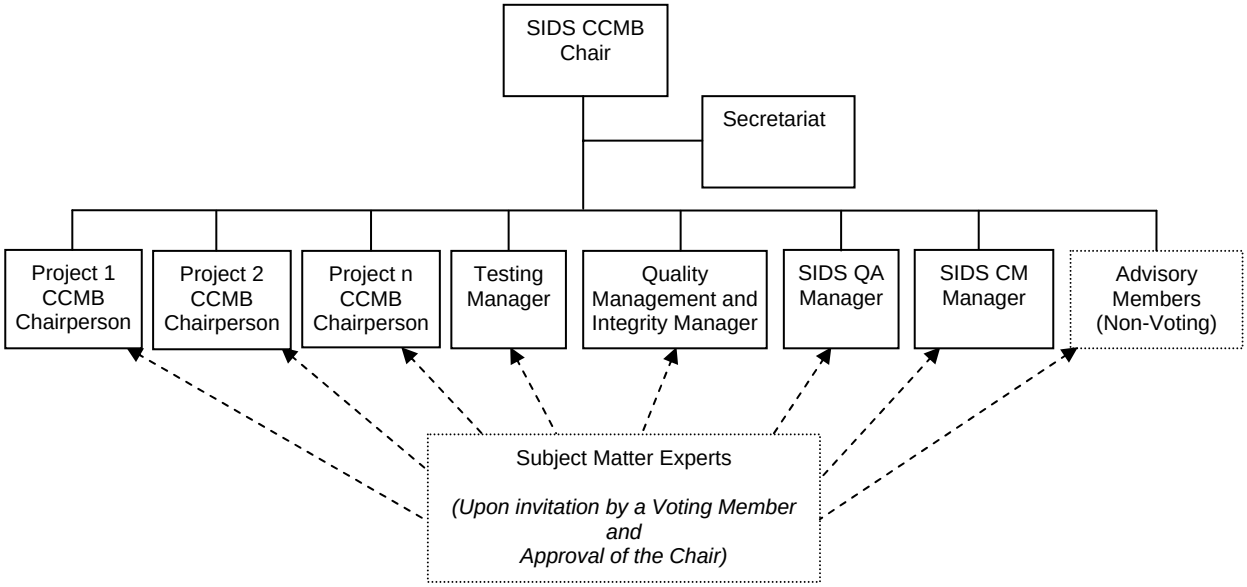


Figure 4 – SIDS CCMB Structure

Specific responsibilities of the SIDS CCMB include, but are not limited to:

- Establish SIDS CCMB rules of conduct.
- Identify and recommend applications and sub-systems for configuration control.
- Determine change priorities and due dates.
- Review and recommend a disposition for all changes to all CI's.
- Recommend dispositions for all proposed requirements and changes thereto.
- Recommend dispositions for SIDS Management publications such as plans, processes, and standard operating procedures.
- Recommend approvals/disapprovals of activity plans.
- Recommend approvals/disapprovals of changes that have impacts on more than one SIDS sub-element (interfaces).
- Review proposed changes from SIDS Branch CCMBs for interface impacts.
- Inform the CM Team and other CM groups of configuration changes that affect the current SIDS configuration standards or other CM organizations

The SIDS CCMB meets on a regularly scheduled basis as determined by the CCMB Chair, but at least quarterly. The CCMB Chair may call meetings out of schedule as needed, especially for Emergency CCPs. The CCMB members review and analyze CCPs and other agenda items and

vote recommendations for the approval or disapproval by the Director, SIDS. The SIDS CCMB Secretariat provides minutes for CCMB meetings (Refer to Section 5.2.1.2).

4.2.2.1. SIDS CCMB Chair

The Director, SIDS, may chair the CCMB or designate a chair from among SIDS senior staff members. The Director, SIDS, will designate a permanent alternate person for those instances when the designated Chair will be unavailable. The alternate will serve in full capacity as Chair only when the appointed CCBB chair is absent with the permission of the Director, SIDS. The Director, SIDS, may not (except as provided by law, specific regulation, or legal absence such as vacation, prolonged illness, or other extended absence from duties) delegate final decision-making responsibilities. All delegations must be in writing and include all SIDS CCMB members as addressees.

The responsibilities of SIDS CCMB Chair include, but are not limited to:

- Convene an Emergency CCMB when necessary,
- Preside at each CCMB meeting,
- Review agenda items,
- Approve CCMB agendas,
- Determine change impacts,
- Assign priorities and due dates,
- Gather member votes and recommendations from CCMB members,
- Assign action items to CCMB members,
- Assign Functional and Physical Configuration Audits and Team Leads,
- Review and approve CCMB minutes prepared by CCMB secretariat,
- Schedule change implementations,
- Sign CCMB recommendations and forward to the Director, SIDS, for approval,
- Defer agenda items to later meetings, and
- Approve and sign CCMB recommendations for items within direct span of authority.[1]
- Ensure compliance with SIDS CCMB rules of conduct.

4.2.2.2. SIDS CCMB Co-Chair

The Manager of the SIDS CM Office (CMO) serves as Administrative Co-chair of SIDS CCMB. The Administrative Co-chair assists the Chair in CCMB procedural matters and in maintaining good order of meeting progress, especially as agenda items are moved between meeting segments (for example, an early agenda item "tabled" until later in the meeting.) In the absence of the CCMB Chair or the designated alternate, the Co-chair has the following responsibilities and authorities:

- Preside over the CCMB meeting,
- Review agenda items,
- Approve the CCMB agenda (if not previously approved),

[1] The CCMB Chair may approve CCMB recommendations only if the Director delegates approval authority and may approve only those items for which such authority has been clearly delegated.

- Request priorities and due dates from the voting members,
- Gather member votes and recommendations from CCMB members,
- Review and approve for signature CCMB minutes prepared by CCMB secretariat, and
- Request schedule change implementations from the voting members.

4.2.2.3. SIDS CCMB Secretariat

The SIDS CCMB Secretariat fulfills the administrative functionality of the CCMB to include, as required, meeting arrangements, agenda preparation, and meeting minutes preparation. The Secretariat is a non-voting member of the CCMB. The Secretariat shall:

- Confirm meeting dates with the CCMB Chair,
- Assist the CCMB Chair with agenda preparation,
- Distribute meeting agendas,
- Distribute CCPs for consideration prior to CCMB meetings,
- Prepare CCMB meeting materials,
- Make facilities preparations for CCMB meetings,
- Attend all CCMB meetings and proceedings,
- Record the proceedings, decisions, and determinations of all CCMB meetings and activities,
- Prepare and distribute draft minutes from CCMB meetings for comments, and
- Distribute approved minutes.

4.2.2.4. SIDS CCMB Voting Members

The SIDS CCMB voting membership is composed of a representative of each major Branch within SIDS. The senior member of each direct sub-organization shall designate an alternate CCMB voting member, who shall attend CCMB meetings when the primary voting member is unavailable. Designated alternates shall have full authority to act in the CCMB on behalf of the sub-organization that he or she represents.

Voting members review proposed changes and modifications to CIs and vote recommendations for approval or disapproval. The minimum SIDS CCMB Voting Members[2] (VA employees only) are:

- SIDS Senior Program Manager (when established)
- SIDS Program Managers for all assigned SIDS Projects (until Sr. Program Manager position is established)
- SIDS Testing Manager
- SIDS Quality Management and Integrity Manager
- SIDS Quality Assurance Manager (Votes on QA issues only)
- SIDS CM Manager (Votes on CM issues only)

Voting member responsibilities include:

[2] The SIDS CCMB voting membership may be modified only upon the recommendation of the board and approval by the Director, SIDS, through the Configuration Change Proposal process.

- Attend each SIDS CCMB meeting,
- Represent the interests of the sub-organization at CCMB meetings and serve as the focal point for all inputs from the sub-organization,
- Ensure thorough review and analysis of CCPs, especially regarding the represented area of interest and expertise,
- Review agenda items before the meeting, determine impacts of proposed actions, and be prepared for discussion,
- Indicate recommendation votes to the Chair,
- Provide internal planning, programming, scheduling, and budgeting information as necessary to the Chair and membership,
- Recommend priorities and due dates,
- Monitor progress on items assigned by Chair,
- Be prepared to advise the CCMB about the status of changes,
- Request the Chair to defer agenda items when appropriate,
- Review CCMB minutes for accuracy, recommend appropriate modifications and vote for or against approvals, and
- Ensure the communication and execution of CCMB discussions and decisions to Branch and team members.

4.2.2.5. SIDS CCMB Advisory Members

SIDS CCMB Advisory Membership consists of representatives from offices both within and outside SIDS. Advisory Members are informed of proposed changes and other items under consideration and requested to advise the CCMB and higher authority about ancillary constraints such as legal, budgetary, operational, resource, etc. Members from outside SIDS are informed of CCPs and meeting times, requested by the Chair (via the Director, SIDS) to attend as appropriate, and receive meeting minutes. Advisory Member analyses should render opinions of "No Impact" or statements explaining a degree of impact along with the provisions impacted.

Advisory membership includes representatives from at least the following groups[3]:

- OI&T Information Technology Operations
- OI&T Office of Cyber and Information Security
- OEAM Enterprise Architecture Services
- OEAM Data Architecture Services

Advisory member responsibilities include (for the organization/function represented):

- Represent organization/function opinions and serve as the focal point for all inputs from the organization,
- Ensure thorough review and analysis of CCPs, especially regarding the represented area of interest and expertise,
- Attend CCMB meetings, when deemed necessary,

[3] The SIDS CCMB cannot mandate attendance of Advisory Members from outside SIDS, but their input can be crucial for ensuring compliance with laws, regulations, security, and budget provisions.

- Advise CCMB membership of organizational/functional considerations/impacts affected by proposed changes,
- Recommend modifications to CCP solutions for compliance with organizational/functional regulations and guidelines,
- Provide Advisory Member opinions on subjects of respective expertise (especially those opinions adverse to the majority Voting Membership),
- Review CCMB minutes for accuracy and recommend appropriate modifications, and
- Ensure the communication and execution of CCMB discussions and decisions to their organization/function members as necessary and appropriate.

4.2.2.6. SIDS CCMB Subject Matter Experts

Voting members of SIDS CCMB may invite Subject Matter Experts (SME) to participate in meetings only when necessary to provide more in-depth technical or operational knowledge about a proposed change under consideration. SME are not regular attendees of CCMB meetings. SME attendance must be requested by a Voting Member or an Advisory Member and approved by the Chair. SME are not allowed to vote on issues before SIDS CCMB.

4.3. SIDS SUB-ORGANIZATION CCMB'S

CCMBs of SIDS sub-organizations (operations and staff elements) and project CCMBs facilitate proactive management control over their respective organizations' assets and systems and help keep decision-making at the lowest appropriate level. Sub-organization CM efforts are responsible for supporting the integrated SIDS enterprise CM system framework and for oversight and guidance for CM efforts at all levels within their respective purviews.

SIDS sub-organizations (except Level F) shall submit a request to establish a CCMB to the next higher level CCMB for analysis and recommendation to its decision-making authority. Requests to establish Level F CCMBs shall be escalated at least to Level D for recommendation and decision. (Refer to Section 4.1.1.) Each CCMB Charter shall delineate the specific responsibility and authority of that CCMB and shall be referenced as the authoritative source in plans and procedures within that organization, except as duly delegated to lower levels. SIDS sub-organization and Project CCMB responsibilities are:

- Exercising management and control over the development and operation of sub-organization technology and management assets in support of SIDS IT enterprise architecture efforts,
- Coordinating and managing technology and management interfaces between or among the internal organizations under its authority and control,
- Ensuring that all assigned technology systems comply with applicable U.S. Government, customer, and security requirements, and
- Properly reviewing and recommending disposition of all modifications or changes to those portions of SIDS technology and management assets under their authority and control.

The roles within each CCMB shall consist of the CCMB Chair, a secretariat, voting members, and, as appropriate, advisory members and subject matter experts.

All CCMB (or equivalent) charters and plans must be forwarded for review and approval by the SIDS CM Office prior to implementation.

4.4. AUTOMATED CONFIGURATION MANAGEMENT APPLICATION

4.4.1. Automated CM Application Criteria

A key requirement of any automated CM application (tool) is a common user interface for accessing CI baselines and CCPs. The ability to view the number and types of baselines and CCPs facilitates identification of duplicate requirements, traceability of requirements through the program lifecycle, and the ability to generate and obtain performance metrics. The automated CM application must meet the following minimum capability criteria:

- Be controllable by a "local" SIDS administrator,
- Allow multiple-user access,
- Provide individual user access security,
- Provide file access security,
- Have multiple file-format capability,
- Have the capability to relate change documents to relevant baseline(s),
- Provide traceability of baseline revisions,
- Provide traceability of baselines from initiation through retirement,
- Track chronologies of change,
- Enable trend analysis,
- Enable links or associations to multiple CI across the enterprise baseline,
- Enable the gathering of performance measures,
- Enable the production of metrics,
- Enable cross-referencing of multiple configuration identifiers,
- Manage change across all platforms, technologies, processes and IT organizations,
- Generate standard and ad-hoc reports, and
- Facilitate disaster recovery.

4.4.2. Automated CM Tool

4.4.2.1. ChangeMan® Dimensions™

SIDS shall employ "ChangeMan® Dimensions™" (Dimensions™) automated CM application (tool) to facilitate development and maintenance of the CM effort, work products, and artifacts within SIDS that meet criteria for complexity, size, importance, cost, and others. Dimensions™ integrates process flow control, change request tracking and version management, enables tracking and reporting CI and CCP progression across multiple programs, and provides the means to measure process participation, manage data, identify trends, and produce various performance measurements and metrics. The tool supports both program management and executive decision-making and can serve as a catalyst for continuous process improvement across SIDS and VA OI&T.

4.4.2.2. TeamTrack

Serena® TeamTrack®[4] is a Web-capable, secure and configurable process & issue management tool that facilitates the establishment and control of standardized business management and product delivery processes. TeamTrack, only upon Rehabilitation Act, Section 508, compliance certification, shall be used within the SIDS CM effort to:

- Establish and enforce SIDS business processes,
- Establish and enforce product life cycle processes,
- Initiate and track CCPs,
- Initiate and track defect reports, and
- Document and track action items.

4.4.2.3. Requirements Traceability Management ®

Serena® Requirements & Traceability Management (RTM®) will be used for tracking and managing requirements throughout a SIDS project lifecycle. RTM databases will be placed under change control within Dimensions or a combination of TeamTrack (upon Section 508 compliance certification) and an approved version control tool. RTM Changes to RTM database requirements may be implemented only upon approval of implementation of a formal CCP that properly addresses the relevant database.

From the top down, new business requirements (System/Subsystem Specification) are received by SIDS typically in some narrative form and entered into the RTM application. An addition, deletion, or modification of a business requirement is deemed to create a discrepancy between business requirements and those in the RTM database. Therefore, a formal CCP is written against the database to incorporate the change, and an RTM Change Request (CR), within the RTM tool, is the means for actually modifying the electronic database. (This last step is to ensure bidirectional traceability for the RTM database change.)

RTM also contains the capability to link requirements-related elements to each business requirement. For example, elements of the System Requirements Specification (sub-requirements), design modules, test scenarios/cases, test data, etc., can all be linked to the appropriate requirement or sub-requirement. The addition, deletion, or modification of any of these elements may be implemented only upon approval of an appropriate CCP. (An RTM CR is the vehicle for implementing the database change.)

4.4.3. Other Tools

Other office automation applications and tools will follow VA standards. If subsequent "upgrades" to the applications and tools used for IT and management CI development are incompatible with the configurations of the items produced, then the relevant versions of the applications and tools will be maintained as part of the configuration of the principle items developed through their use.

[4] TeamTrack® is a registered trademark of Serena Software, Inc.

4.5. CONFIGURATION MANAGEMENT LIBRARY

The SIDS Configuration Management Library (CML) is maintained as a distinct, separate, and autonomous entity that is generally for the development of a work product (application, database, management documents). A product, when ready for deployment (publication, installation, or other issuance) and properly authorized, is copied from the CML to its operational environment for use by its intended audience. The CML also provides record copies of all formal materials (to Records Management), file backups and file restorations (for disaster recovery).

The SIDS CML is the collective repository for all controlled baselines (Refer to Terms and Definitions) of SIDS management publications, SIDS IT documentation, SIDS-generated work products (such as requirements, designs, diagrams, applications, databases, etc.) and selected external documentation. CML contents are accessible to development or maintenance personnel typically through use of the CM toolset. Upon appropriate authorization, baselines are moved through the library process and deployed (issued or published as a version.release) into the operational environment (for installation onto operational platforms or for availability to intended users (the Process Asset Library or Technical Library). (Refer to the "SIDS CML User Guide" – TBD.)

The CML custodian is responsible for the storage and maintenance of all formal materials related to all systems, subsystems and applications designated by SIDS CCMB as Configuration Items (CIs). The CML custodian conducts storage and maintenance, maintains the secure environment, controls access, and ensures proper administration of the baseline change process.

4.5.1. CML Baseline Submittals

Upon receiving authorization through/from the SIDS CCMB, the CML custodian installs initial files of CI into the tool and controls update, maintenance, and reader access through the capabilities of the CM tool. CM personnel assist authorized individuals in obtaining access to baseline and change management capabilities. The originator of new CI files shall notify the CM custodian in writing (electronic or hard copy) that a submittal has been provided and includes the necessary specific information about the item to ensure its unique identification.

Upon receipt of submittal notification, the CM custodian shall verify the inclusion of the correct contents (with the assistance of the Quality Assurance (QA) representative if necessary or required by authorizing authority) and identifier and place the item in the appropriate baseline directory or subdirectory.*****

*** NOTE:** *From this point forward, no modification to a baseline may be made without going through the CCM Process.*

4.5.2. Configuration Management Library Maintenance

The CML custodian maintains the CML in a secure environment with controlled access. The CML comprises all controlled records and materials for all CI throughout the life cycle of the CI, from the initial request for a system/subsystem or application through its proper retirement. The CM Office holds, exercises ownership over, and maintains all CM directories, subdirectories,

and files in electronic media and, if necessary and possible, hardcopy media for the Director, SIDS.

The CML is the single source for controlled copies of CI baselines and related materials and serves to protect the official operational baseline while accommodating the work requirements of the organization and sub-organizations. Copies of baselines and materials outside the CML are not controlled and should be verified with CML holdings before using them as the basis for further work. Individuals or teams may obtain copies of baselines for further work as directed by CML procedures, user guides, and handbooks.

4.5.3. Backup And Restore

To ensure that valid copies of CM files, databases, data, and automated tools are stored in and available for timely retrieval from a secure environment in the event of a catastrophe, backups are required on SIDS CM servers. The SIDS CM servers are maintained in the Office of Information Technology Operations, which performs the necessary backups in accordance with that Office's procedures (minimally, backups of all *changed* server contents ("deltas") nightly and full backups weekly).

4.5.4. Removals and Archives

Direction from higher authority or requests to remove obsolete or discontinued SIDS products systems, subsystems, or applications from VA OI&T or SIDS systems shall be submitted and acted upon in accordance with the CCM process. (Refer to Section 5.3., below.) Superseded and retired artifacts and work products under the responsibility of SIDS shall be placed in archives and retained in accordance with Federal regulations or for seven (7) years, whichever is greater. Materials to be archived include but are not limited to:

- Superseded versions/releases of active CI,
- Tools (CM, build, assembler, compiler tools and others) necessary to handle files and materials that are being archived,
- All CCM records pertaining to the CI, and
- All management work products and artifacts such as minutes, measurement reports, performance data reports, etc.

An archived application, database, or tool shall be retained longer than seven years if it is needed to "read" work products that remain in operation beyond that time, or if Department of Veterans Affairs Records Collection and Retention Policies so dictates.

4.6. CM TRAINING

SIDS CM group will provide CM orientation and training to SIDS-level managers and SIDS personnel to include, but not limited to:

- Members of the CCMB,
- Associated SIDS organization members,
- Developers, testers, reviewers, etc., of SIDS-level products.

The SIDS CM Manager shall ensure that all members of the CM group have the necessary skills or are trained to conduct their CM duties. The SIDS CM group, with the approval of the Director, SIDS, (or delegated authority) will identify subjects for training, prepare training materials, conduct or facilitate the training, and report or maintain records of training as appropriate.

5. SIDS CM ACTIVITIES AND OPERATIONS

5.1. CM ACTIVITY RELATIONSHIPS

The VA standard, Electronic Industries Alliance (EIA)/Government Electronic and Information Technology Association (GEIA)) Standard-649-A, National Consensus Standard for Configuration Management, April 2004, enumerates five distinct CM functions consisting of the following activities and operations:

a. **Configuration Management Planning and Management** – serves to establish CM activities for the context and environment in which CM is to be performed. Planning and management establish the foundation from which the CM discipline is exercised.

b. **Configuration Identification** – forms "… the basis from which the configuration of products is defined and approved; products and documents are labeled; changes are managed; and accountability is maintained throughout the product life cycle."[5] Configuration identification is the function of determining exactly which products or sub-products are to be subjected to the formality of the CM discipline.

c. **Configuration Change Management** –the "function for (controlling) changes and variances to a product using a systematic, measurable change process."[6] CCM, the most visible function, is the means by which changes to identified items are submitted, approved, incorporated, and implemented in a prescribed and controlled manner.

d. **Configuration Status Accounting** – provides an accurate, timely information base concerning items under formal configuration control throughout the life cycle of the product and constitutes a large part of the CM tracking system.

e. **Configuration Verification and Audit** – confirms that what has been built fulfills functional and physical product requirements, designs, and specifications.

Configuration management planning and management addresses, at minimum:

- Roles and responsibilities for CM processes;
- Procedures for conducting CM functions;
- CM training to ensure that individuals understand CM procedures and their responsibilities, authority, and accountability;
- Performance measurements addressing CM planning and procedural effectiveness;
- Monitoring CM as provided by suppliers;
- Planning for sharing configuration information; and
- Preservation of digital data records of configuration information.

[5] Government Electronics and Information Technology Association (Electronic Industries Alliance) Standard 649, National Consensus Standard for Configuration Management, April 2004, p. 16
[6] Ibid, p. 22

Configuration identification consists of:

- Determining and defining product attributes (such as performance, functional, and physical),
- Determining the structure of the product (typically by decomposing the product into its component parts and organizing them according to relationships,
- Uniquely identifying each part selected for formal configuration control (typically by assigning unique identifiers),
- Establishing an initial baseline for each controlled component (at a point in time from which changes will be addressed), and
- Identifying interfaces between two or more elements in terms of attributes, ownership, and responsibility.

Configuration change management helps ensure:

- Proper maintenance and control of configuration baselines;
- Consistent configurations and configuration information;
- Orderly communication of change information;
- Proper evaluation of cost, savings, and alternative change trade-offs;
- Change decisions are based on knowledge of complete change impact(s);
- Limitation of changes to those which are necessary or offer significant benefit;
- Consideration of customer and user interests;
- Proper control of interfaces;
- Proper documentation and control of variances; and
- Continued supportability of products after change.

High-level components of CCM include:

- Identifying the need for a change;
- Defining the change;
- Determining and defining change impacts;
- Evaluating and coordinating the proposed change;
- Incorporating approved changes in the product and related configuration information;
- Verifying change incorporation and continued consistency with configuration information; and
- Identifying, documenting, approving, and implementing variances from baseline requirements.

Configuration status accounting helps ensure:

- The capture of product and product configuration information data throughout the product life cycle;
- The ability to retrieve current, accurate information concerning such matters as change decisions, design changes, design problem investigations, warranties, shelf-life calculations, and operating-life calculations;
- Access to complete product configuration information, current or past; and

- Historical traceability of product configurations and product configuration information, including changes.[7]

Configuration verification and audits serve to:

- Ensure that designs provide the agreed-to performance capabilities,
- Validate the integrity of the configuration information,
- Verify consistency between the product and its configuration information,
- Validate the adequacy of the processes for providing continuous control of configurations,
- Provide confidence that product definition information is under proper control, and
- Ensure that a controlled configuration is the basis for operation and maintenance instructions, training, spare and repair parts, etc.[8]

5.2. CM PLANNING

This plan and corresponding policies, charters, procedures, and instructions constitute CM Planning for the SIDS organization.

5.3. CONFIGURATION IDENTIFICATION

Configuration identification, the first major step in establishing configuration control over a configuration item (CI), refers to the process of selecting items and elements to be placed under formal CCM, designating the technical documentation (specifications, drawings, manuals, and operational procedures) that will describe those items and elements and their owners, and applying unique identifiers to the items, components, elements and documentation. After a CI has been properly identified, the identification information is ready for baseline establishment and management.

5.3.1. Configuration Item Discussion

"Configuration Item" (CI) is defined as a work product or aggregation of work products (hardware, software, firmware, documentation, or any discrete portions) designated for CCM and treated as a single entity in the CM process. Configuration items can be decomposed into configuration components, units, modules, elements, or other sub-pieces. More generically, "configuration item" refers to any piece or sub-piece that has been designated by proper authority for formal CCM.

Items identified by the SIDS CCMB and approved by the Director, SIDS, or mandated by the Director or higher authority will be placed under configuration control at the Director, SIDS, level unless control is delegated to a subordinate level. Items for configuration control will include:

- SIDS Management plans, processes, and procedures for SIDS Operations (CM, QA, Requirements Management, Risk Management, etc.),

[7] Ibid, p. 29
[8] Ibid, p. 32

- CM Tools,
- Hardware Requirements Specifications for SIDS level hardware,
- Materials having impact between two or more direct-report sub-organizations, and
- Other related documentation used in satisfying SIDS mission.

5.3.2. Configuration Item Selection

CI selection is the determination that a particular item or set of items is to be placed under formal CCM. The SIDS CCMB may select assigned SIDS assets that include, but are not limited to: hardware, networks, software, databases, Web assets, Modified-(Commercial)-Off-The-Shelf (MOTS), documentation and publications, and IDE assets.

SIDS has established criteria to consider when selecting and nominating an item for formal configuration control. Selection may be based on a major impact on one criteria or an accumulation of multiple small impacts. Selection criteria address such characteristics as:

- Criticality
- Complexity
- Cost
- Risk of failure
- Impact of failure
- Interfaces
- Multiplicity of uses
- Geographic Diversity

Any member of the SIDS organization may nominate a CI through the CCM process described in Section 5.4., Configuration Change Management. Additionally, the Director, SIDS, (or higher authority) may direct that items be placed under formal CCM. (Refer to "SIDS Configuration Item Selection Procedure" for selection criteria.)

5.3.3. Configuration Item Definition

"CI Definition" is the decomposition of the CI into the components and attributes to be included in the CI package, the release authorities (or owners), and the controlling CCMB. Examples of decomposition are: (1) a data *system* CI with a listing of all the component "databases" that interact, tables, and possibly the network and hardware on which they operate, manuals, etc.; (2) a network CI with a listing of all the hardware components (including specifications and connection schematics), operating systems, and applications; or (3) a software application CI that includes the base program source code, source code for modules, executables, user's manual, installation manual, training materials, etc.

When proposing or requesting a new CI, an individual works with the CM group to ensure that the CI is decomposed to an appropriate level of detail. The proposal is then forwarded to the Director, SIDS, through SIDS CCMB. The CCMB uses established criteria to consider the recommendation for approval/disapproval of a CI definition. (Refer to "CI Definition Procedure.")

5.3.4. Configuration Item Identifiers

CI identifiers are unique alphanumeric streams attached to each CI, its component parts, and the iterations. Thus, a properly developed identifier provides the means for referencing a specific item and for relating it with its descriptive documentation. CI identifiers provide the data necessary for quickly and accurately selecting a specific CI and its components (down to the revision or version/release level) upon which work is to be performed.

Each stand-alone document must have a unique identifier (as does each piece of configuration documentation) to associate it correctly with the configuration of the item to which it relates. Additionally, respective digital files for each version of each representation and its component files must be uniquely identified and managed. The file names for digital file formats of CI include the elements above. The responsible manager (with the assistance of the CM group) assembles the CI identifier(s). (Refer to "CI Identifier Procedure.")

5.3.5. Configuration Baselines

Baselines are central to an effective CM program and establishing a known and defined point of reference is central to an effective management process. "A configuration baseline consists of the product definition information that defines and describes the agreed to product attributes at a specific time."[9] A baseline is a "snapshot-in-time" of a system or subsystem (including all system or subsystem components and elements), a component, or an element.

A baseline identifies a known configuration from which further work can continue and to which changes can be addressed. A baseline exists at any point in time, but formally required configuration baselines may be required and are usually linked to the phases or stages of a defined process such as a system development life cycle (SDLC). At gateway reviews for transition from one process stage to the next, audits of the "current" baseline are taken to ensure compliance with product requirements and phase or stage requirements.

The "customer" and responsible SIDS personnel, with the applicable project manager, QA, CM, and other functional leads, determine the required reviews and the specific baseline contents. The specific reviews selected will be named and described in the project plan. Appendix B describes some of the reviews and formal baselines that SIDS projects may require.

5.3.5.1. Initial Baselines

The "List of SIDS CCMB Configuration Items" ("List") shall be the initial baseline for SIDS. The "List" is a baseline of all CI placed under formal CCM within SIDS. Submittal of a new item for inclusion in the "List" will identify the CI in terms of its project or product name, release authority (or owner), and the controlling CCMB. The submittal also will be accompanied by "definition" information, if available, such as components, elements and deliverables of the product package.

[9] Ibid, p. 20. Further, "time" as used in this paragraph may be chronologically or event-driven. A chronological point in time would refer to a date and time. Completion of a procedural step or an SDLC stage or phase is an example of an event-driven point in time.

Upon approval of this CM Plan, the form and format of the "List" shall be developed under the auspices of SIDS CCMB and submitted through the CCM process to the Director, SIDS, for approval. (Refer to Section 5.4., Configuration Change Management.) Upon approval by the Director, SIDS, the "List of SIDS CCMB Configuration Items" will be a CI in form, format, and content. Changes and modifications to the "List" may occur only through the formal CCP process. The approval authority for changes to the "List" resides with the Director, SIDS (or SIDS-delegated authority). Revisions or version/release numbers for the "List" will be incremented if a change affects the form or its format. Versions with updated content will be identified by the date.

The addition or deletion of an initial CI baseline for a product or component shall be nominated for the "List" through the preparation of a CCP. The originator shall attach to the proposal all available product identification and definition information including, but not limited to:

- Configuration identification information for the proposed CI,
- All known configuration components and elements to be formally managed,
- The respective owners, and
- An estimate of when the first work products and artifacts are scheduled for formal management and control.

Assigned CM personnel will assist the proposal originator in developing the attachment material for the CCP form and use the information to begin setting up the product/project in the CML.

The CCMB, after proper analysis to ensure appropriateness, completeness, and accuracy of the CCP and attachments, shall recommend its approval/disapproval through the CCM process. (Refer to Section 5.4.) The SIDS CCMB shall consider only those items for which it holds direct authority, as indicated in Section 4.2. During analysis and discussion of the proposal, the CCMB or Director, SIDS, may:

- Accept the proposal as presented,
- Desire or require clarification of or additional information about the proposal prior to approval/disapproval recommendation, or
- Accept the proposal with the proviso that additional proposals be submitted against the item after incorporation into the "List."

5.3.5.2. Baseline Maintenance

The CM Specialist/Secretariat, using the assigned CM tools, shall ensure that baselines (including historical revisions) are maintained and that only authorized baselines are released.

5.3.5.2.1. Revision Control

A *revision* is an updated baseline that is retained internally by the group or team developing it. A baseline may undergo several revisions before it is released to a design phase. Further, the use of revisions facilitates the management of parallel or branch development efforts. A *release* differs from a revision in that a release may refer to the baseline that is distributed for use in the next phase of the product life cycle. A *version*, in this context, is a special release into an operational

environment (or production). Many revisions of components and elements may take place before a new version is issued, especially if the work product is complex, involves a large number of workers, or has an established release schedule.

The project/product CM Specialist or CML custodian is responsible for maintaining revision control. Dimensions™ features a "trunk and branches" approach to baseline revisions for complex development efforts. Using appropriate CM tools, the CM Specialist shall ensure that the revision number of a modified baseline file "checked in" to the CM system is properly incremented and retain all revisions for change traceability.

Copies of all superseded revisions are retained in the CML as an audit trail or to provide an older baseline if needed for further work. (Refer to "Archiving" below.)

5.3.5.2.2. Version/Release Control

Typically, products distributed for use follow a version is an identified product baseline or body of baseline components, including the appropriate documents and documentation, intended for distribution/installation and use by the organizational community at large. To help alleviate possible confusion by the user, all components of the new version will be labeled with the same version number. If a component was not modified for the new release, labels shall be affixed to the appropriate revision to indicate the release(s) to which the file was assigned. (Labels are electronic features of Dimensions™ files.)

Note: In the context of this subsection, "release" refers to a subset of a version.

For a new or updated release, the system/sub-system manager includes a description of all included CCPs, their effects on the use of the system/sub-system, and the identity of changes that require user training. The totality of the CI package is a version/release, which is documented in a Product Version Description (PVD) that accompanies the CI when it is issued.

The CM Office shall issue new version/release files and materials only by authority of the Director, SIDS, upon the recommendation of the SIDS CCMB, which has the responsibility for ensuring that all files and materials meet established requirements. When promulgation is required, the CM Office will assemble the designated components of the version/release package, verify the contents with the Release Manager and Quality Assurance specialist, and release the package for installation/distribution.

The CM Office will retain in the CML copies of all versions/releases for purposes of audit trails or for the possibility that older versions may be needed in the future. (Refer to "Archiving" below.)

5.4. CONFIGURATION CHANGE MANAGEMENT

CCM is the means by which the integrity of approved configurations is maintained. CCM is the control and tracking of changes and baselines. The exercise of proper CCM facilitates the accurate incorporation and implementation of approved changes to a CI baseline to meet the CM requirements and principles stated in Section 5.1.

Through a systematic sequence of evaluation, coordination, and formal disposition of proposed changes, the CCP process ensures that changes are fully analyzed, understood, and agreed upon before they are incorporated and implemented, and that all components reflect the agreed-upon changes.

Proper revision control ensures accurate, internal accounting for development and change efforts involving multiple persons (especially those working on multiple parts of a baseline). Revision control is particularly important in but is not limited to the practice of "scheduled releases."

5.4.1. Configuration Change Proposal

The CCP is the mechanism used to recommend, approve, incorporate and implement changes to all baselines under direct formal SIDS configuration control. CCP processes provide the means for:

- Proposing identified needs for change,
- Defining the change,
- Documenting change impacts,
- Evaluating and coordinating proposed changes,
- Incorporating approved changes in the product/system and its related product/system configuration information,
- Verifying change incorporation and continued consistency with the product configuration information, and
- Identifying, documenting, approving, and implementing variances from product-requirements baselines.[10]

The Figure 5 (next page) outlines the CCP process flow to provide an overview of the types of activities that occur in its steps. (Refer to the CCP Preparation and Life Cycle Procedure –TBD.) Figure 5 indicates a linear flow, but it is important to note that a CCP may be returned to a previous step for rework.

Each CCP decision reached at one level of the CM structure is reviewed at the next higher level prior to implementation. The SIDS CCMB will determine the format it requires for review (minimum sub-organization CCMB meeting minutes – other formats include each CCP, summary report of sub-organization CCPs, or other). These reviews will serve as a check on identifying changes that may impact across sub-elements, projects and management groups or to ensure application of appropriate decision-making authority. If the review reveals an interface impact, then the SIDS CCMB assumes review and decision authority. If the review reveals such an interface between SIDS and an element of any other equivalent level CCMB functional body, SIDS will escalate the matter to higher authority.

It is important to document even minor changes to establish a configuration audit trail to help resolve product failures or questions and to help ensure compliance with the Clinger-Cohen Act

[10] Ibid, p. 22

of 1996. In many cases, the slightly higher cost of a comprehensive CCM process will more than offset the cost of reconstructing an audit trail.

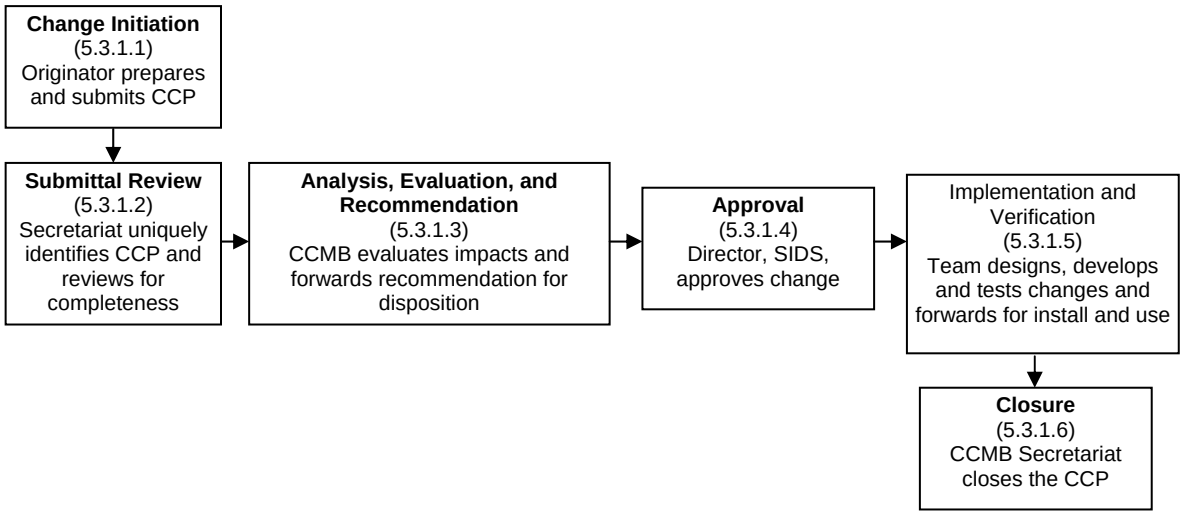


Figure 4 – General Life Cycle for Configuration Change Proposal

5.4.1.1. Change Initiation

Submittal of a CCP initiates the CCP tracking process. Anyone may initiate a CCP into the SIDS change proposal life cycle. All who have access to the CM tools may enter a CCP into the system directly. CCMB members may initiate CCPs for those not having access to the CM tool. However, all changes to SIDS-controlled system or sub-system baselines must be authorized by the CCMB through the CCP process.

The need for a change may result from several stimuli including, but not limited to:

- New requirements from the customer or owner,
- A change to existing requirements,
- An enhancement (suggestion for improvement),
- Integration of systems or sub-systems,
- A solution to a Discrepancy Report, Problem Report, or Trouble Ticket (Refer to Appendix C, Change Document Relationships), or
- Observed malfunctions.

NOTE: *A Discrepancy Report (DR), Testing Problem Report (TPR or PR), Test Incident Report (TIR), Trouble Ticket (TT), or a CCP may spawn a new CCP. A CCP never spawns the former.*

The two major aspects of initiating a proposed change are 1) documenting the change and 2) determining the change classification. Documenting the change includes, but is not limited to:

- Uniquely identifying the change (which is done by the CM tool),
- Identifying the originator and their organization,
- Indicating the priority or urgency,

- Identifying all affected product(s) (including components and interfaces),
- Applying an appropriate subject or title,
- Describing the change and its scope (includes effects on specified performance, operation, maintenance, servicing, training, repair parts, support and testing equipment, etc.,
- Product configuration information affected by the change,
- Justification or reason for the change,
- Consequences of not making the change,
- Extent of the change (which parts, components, etc. will be changed),
- Estimate of cost or savings,
- Schedule for implementation,
- Schedule for delivery, and
- Criteria for retrofitting (if any).

All information may not be available upon initial submittal of the proposed change or upon first introduction to the CCMB, but should be included and analyzed before the CCMB makes its recommendation to the Director, SIDS. In practice, much of this information may be provided, expanded, or expounded upon during analysis and evaluation of the CCP by the CCMB membership and their analysts. The CCMB must provide the Director, SIDS, a written explanation of the absence of any of the above. Whenever possible, change pages (i.e., marked up copies of documents, source code listings, diagrams, etc.) should be attached to the CCP to illustrate the exact change proposed (Refer to "CCP Initiation Procedure" for greater detail—TBD).

5.4.1.2. Administrative Review

Before sending the CCP to the CCB membership, the Secretariat performs an administrative review (Refer to the CCP Administrative Review Procedure – TBD.):

- To determine if the proposed change is an emergency,
- To determine whether the CCP duplicates a previous entry,
- To verify the priority or urgency,
- To ensure appropriateness of the title or subject,
- To determine if any information needs further clarification, and
- To ensure that the CCP is forwarded appropriately for analysis, evaluation, and disposition recommendation.

If the CCP has been marked as an emergency or if the Secretariat thinks it should be an emergency, the Secretariat consults with the CCMB Chair to verify the handling to be employed.

5.4.1.3. Analysis, Evaluation, and Recommendation

After the administrative review, the CCMB membership receives the CCP. Members analyze and evaluate the CCP problem and proposed solution to define as clearly and precisely as possible all characteristics affected by the proposed change including but not limited to:

- Necessity for the change,
- Necessity for emergency handling,
- Affected components, parts and interfaces,
- Impacts assessments on the identified components, parts and interfaces,
- Costs/savings, and
- Schedule considerations.

If the CCP was submitted without a solution and the CCMB determines that a change is necessary, the CCMB members prepare one or more solutions for consideration (possibly by submitting the problem to their subject matter experts). If an analyst/evaluator perceives a necessity for emergency handling, the representative member notifies the CCMB Chair and Secretariat immediately for verification. An emergency requires special handling as discussed in Section 5.3.2., below.

During the Analysis, Evaluation, and Recommendation step, the CCP may be deferred, redistributed and reconsidered over the course of several meetings until the CCMB has determined there is sufficient information and votes a recommendation for disposition.

After analyzing and evaluating the CCP, the CCMB votes to recommend approval/disapproval of the change. The majority vote of the voting membership determines the recommendation to be forwarded. Recommendations for disapproval and dissenting votes from approval recommendations must be documented and accompanied by comments of justification. Advisory members, even though they may not vote, may and should make dissenting comments if warranted.[11] Documented comments ensure that the Director, SIDS, has all the information needed to make the appropriate decision. Before making that decision, the Director may return the CCP to the CCMB for additional information (in an iterative process).

5.4.1.4. Approval

Final approval/disapproval of a change is reserved to the Director, SIDS, or higher authority. The Director reviews the CCP recommendation and dissenting opinions, and determines the proper authority level. If the change is within the Director's authority, the Director may:

1. Request further information from the CCB,
2. Approve the change for implementation or further work,
3. Determine that decision authority is at a higher level and escalate the proposal, or
4. Determine that the change has impacts outside SIDS and requires consideration with other organizations and escalate the proposal.

(It is especially important to note that an *approved* CCP is not simply permission to correct or change something, but acceptance of an exact, defined solution to the problem, enhancement, or issue. The solution is often an attachment to the CCP due to length or the necessity for change pages.)

[11] For example, when a change is recommended for approval but a financial officer (advisory member) needs to inform the VA CIO of budgetary constraints.

5.4.1.4.1. Escalation

The SIDS CCMB (Level C, refer to Section 4.1.1.) is chartered to review and recommend approval/disapproval of CCPs affecting interfaces between SIDS entities and systems and external entities and systems. If a proposed change exceeds the Director's threshold of authority, the Director escalates the CCP to higher authority with the recommendation and background information. If the CCP is determined to have impacts outside SIDS, the Director will, in accordance with direction from higher authority and prior to approval for further work, either escalate the CCP with recommendation to the higher authority or forward it to other appropriate authorities for consideration and coordination. (Refer to the "CCP Escalation Procedure" – TBD.)

SIDS organizations at Levels E and F will follow similar CCP escalation protocols to their respective Level D CCMBs.

5.4.1.4.2. CCP Decision Reviews

Decisions on CCPs from each level of authority within the SIDS are conducted to ensure proper coordination of those issues and topics that have impacts across more than one organization/sub-organization and to ensure decision making at the most appropriate level.

CCPs escalated to the SIDS CCMB will be evaluated and a disposition recommended to the Director for decision as if the CCP were newly originated at the SIDS level.

Documentation for CCPs *approved* at Level D shall be forwarded to the SIDS CCMB for review. (The SIDS CCMB will determine the form of documentation to be forwarded, but the minimum requirement is CCMB minutes.) Each CCP is reviewed for interface impacts and authority-threshold. If the review indicates that decision authority is reserved to the Director, SIDS, or a higher authority, the Director will inform the Level D authority and direct that implementation be placed on hold. The Director will then place the CCP on the SIDS CCMB meeting agenda or escalate higher, whichever is appropriate. If there is an interface impact, the SIDS CCMB Chair will direct that the CCP be placed on the SIDS CCMB meeting agenda and notify the Level D authority to place implementation on hold. If the SIDS CCMB determines that there is no impact across sub-organizations or to a higher level organization, the SIDS CCMB Chair will notify the Level D authority that they may continue according to normal procedures.

SIDS organizations at Levels E and F will follow similar CCP escalation protocols to their respective Level D and E CCMBs.

5.4.1.5. Implementation and Verification

Implementation and verification, involving multiple activities begins after the Director, SIDS, approves a solution. Implementation and verification includes incorporation and integration of the solution, testing/review/editing (unit, system, regression, etc.), auditing, acceptance, installation, and, if a change to an operational system, commencement of operations.

5.4.1.6. Closure

Upon verification that a change has been successfully implemented, the CM Specialist ensures closure of the CCP within the CM tool and notifies the CCMB membership.

5.4.2. Emergency Configuration Change Proposals

Special provisions apply when corrective action is required for a problem categorized as a catastrophic event, past or imminent. A catastrophic event is one that has caused damage to the system or a severe work stoppage. An imminent catastrophic event is one that would cause such damage and is deemed to require corrective action to be initiated within 48 hours or less (Refer to the SIDS "Emergency CCP Procedure" for further detail—TBD).

If a catastrophic event has occurred, appropriate personnel should resolve the problem and then file an Emergency CCP to document the action taken. This filing serves four primary purposes:

- Documents a change to the system and updates the baseline information,
- Gives the CCMB an opportunity to determine the best solution for the longer term,
- Provides an opportunity to determine if changes are necessary for other elements or components, and
- Ensures an unbroken audit trail for traceability.

If a catastrophic event has occurred or is identified as imminent prior to CCP submittal, the originator should indicate that it is an Emergency CCP when it is submitted. If a CCP is identified as or suspected to be an Emergency subsequent to submittal, the identifier should notify the CM Specialist and the CCMB Chair immediately.

Upon receipt of an Emergency CCP or determination that a normal CCP warrants emergency handling, the CCMB Secretariat will immediately notify the CCB Chair for verification of the requirement for emergency handling. If warranted, the Chair will convene and conduct an Emergency CCMB by the most convenient means available. (Refer to SIDS "Emergency CCP Procedure" – TBD)

NOTE: *Under emergency conditions, the solution employed may be a "quick fix," a "stop-gap," or a "work-around" and not the best solution for the longer term. After the emergency has been addressed, the CCMB must carefully reconsider the CCP and the solution employed to: 1) determine whether the best solution was employed, 2) determine the best solution if the best solution was not employed, and 3) determine other impacted elements, components, or organizations, and other CCPs required because of the solution. (If the solution is deemed less than the best, another CCP will be warranted.)*

5.5. CONFIGURATION STATUS ACCOUNTING AND REPORTING

5.5.1. Status Accounting

The Configuration Status Accounting (CSA) activity includes recording, storing, and reporting baseline evolutions and implementation status information:

- To ensure the capability to retrieve complete, current, and accurate information concerning change decisions, design changes, investigations of design problems, warranties, shelf-life calculations, and operating-life calculations;
- To ensure that complete product configuration information can be accessed;
- To provide historical traceability of the product configuration and configuration information; and
- To record data that can be gathered and reported for better project management, control, and coordination.

The SIDS CMO is responsible for ensuring that accurate, complete, and timely CSA data is maintained. CSA data includes:

- Technical data comprising the configuration identification,
- Essential configuration elements,
- Current version/release/revision of each configuration item under configuration control,
- Required contractual information to be included in the records/reports for each configuration item, and
- Change data and status information about proposed changes to the configuration including:

    - Specific identification of CCPs,
    - Specific identification of the relevant CI(s),
    - Incorporation/implementation data on CCPs,
    - The activity responsible for development and implementation, and
    - Disposition status of changes

CSA has the following characteristics:

- CSA begins with the submittal of the configuration identification of CI and the related descriptive documentation.
- CSA provides an accurate, timely information base concerning a product and associated product configuration information throughout the product life cycle.
- CSA provides visibility into the current baseline, and traceability of approved and pending changes to the baseline.
- CSA ensures that current and historical configurations can be accurately determined throughout the life cycle by capturing and maintaining product configuration and product change information on an as-occurring basis.

5.6. AUDITING

The intent of configuration audits is to determine the extent to which the as-designed/as-tested/as-built product reflects the functional and physical characteristics specified in the product requirements. Functional Configuration Audits (FCA) and Physical Configuration Audits (PCA) are performed on operational and development baselines and other deliverables specified and defined as CI, be they hardware, software, documentation, or other specified items and assets.

Operational baseline systems are audited to ensure that they are using the latest approved baselines and that the approved configurations are correct. Operational baseline audits are performed by one or more CM personnel, QA representation, and the affected project, operations, or application managers. Initially, SIDS audits shall be conducted on all operational assets for which SIDS is responsible. As the collection of assets becomes more numerous and complex, the Director, SIDS, may consent to a reduction in the scope of audits. A reduction in scope notwithstanding, the minimum audit requirements for each audit event are:

- At least semi-annually,
- A minimum of two projects or areas of VA business functionality (selected on a random basis),
- A minimum of ten percent (10%) of those OI&T operational subsystems for which SIDS is responsible, and
- A minimum of twenty-five percent (25%) of SIDS management documentation (CM, QA, Requirements Management, etc., selected on a random basis).

During development of SIDS management and production products and projects baselines are audited incrementally at review "gateways" to ensure that they have met the exit criteria for passage into the next phase of the development life cycle. These audits, conducted by a peer review group described below, may be included as part of the minimum auditing requirements in the preceding paragraph. The minimum exit and entry criteria for development phases of each product/project will be specified according to the SIDS system development life cycle.

The CM group, with the owner(s), product/project managers, QA representative, and other assigned audit team members, conducts audits for each review or test to make sure that all deliverables requirements are met. The CM group maintains all audit materials under strict controls to minimize the effort required for the audit team. Appendix B contains a listing of reviews available for assignment by the Director, SIDS, or product/project manager. The Director, SIDS, or product/project manager may call for other reviews.

5.6.1. Functional Configuration Audit

The FCA objective is to verify that all tests/reviews for a baseline have been completed and that performance (based upon the test/review results) meets the specified performance requirements of the baseline. The SIDS CCMB Chair directs the formation and composition of each FCA team and appoints the FCA Team Lead. The assigned FCA Team Lead, assisted by the CM specialist, is responsible for coordinating the FCA and ensuring that:

- All materials are supplied,
- An agenda is published,
- Results are recorded and reported,
- Action items are recorded and tracked to resolution, and
- Action item status reports are issued.

The FCA Team Lead prepares a report at the conclusion of the FCA, a copy of which is retained in the CML System. Using the report, the CCMB Chair will assign action items to correct

reported deficiencies or discrepancies. (Refer to the SIDS "Functional Configuration Audit Procedure")

5.6.2. Physical Configuration Audit

A Physical Configuration Audit (PCA) serves to verify that the documentation representing the product matches the product design in adequacy, completeness, and accuracy. The audit may be done in two parts, one to compare product definition information to the design information and one to compare the product definition information to the product operational information. The combination of the two parts creates a triangular verification trail from "what was intended" to "what was specified" to "what was built." The SIDS CCMB Chair directs the formation and composition of each PCA and appoints the PCA Team Lead. The PCA Team Lead, assisted by the CM specialist, is responsible for coordinating the PCA and ensuring that:

- Audits are planned and prepared for,
- Designated baselines are available,
- Results are recorded and reported,
- Action items are recorded and tracked to resolution, and
- Action item status reports are issued.

The PCA Team Lead prepares a report at the conclusion of the PCA (a copy is retained in the CML System). The CCMB Chair will assign action items to correct reported deficiencies or discrepancies. (Refer to the "SIDS Physical Configuration Audit Procedure")

5.6.3. Configuration Audit Roles and Responsibilities

The following roles and responsibilities are to be used unless and until assigned SIDS Quality Assurance personnel develop SIDS roles and responsibilities for audits.

5.6.3.1. SIDS CCMB Chair

SIDS CCMB Chair responsibilities for Configuration Audits are to:

- Assign the Team Lead and membership of each FCA/PCA team,
- Review FCA/PCA reports,
- Assign action items from FCA/PCA reports to CCMB members,
- Ensure that action items resulting from configuration audits are completed, and
- Direct final FCA/PCA Report submittal in accordance with contract requirements.

5.6.3.2. CM Specialist

The CM Specialist configuration audit responsibilities may include, but are not limited to:

- Provide administrative direction and act as coordinator,
- Assist SIDS CCMB Chair and development managers to determine audit schedules,
- Assist with FCA/PCA plan preparation,
- Coordinate all administrative and technical materials for team use,
- Record action items discovered by the FCA/PCA team,

- Collect and retain forms and checklists completed by the team,
- Assist the FCA/PCA Team Lead with consolidation of action items and preparation of FCA/PCA reports, and
- Track FCA/PCA action items until closure.

5.6.3.3. FCA/PCA Team Lead

FCA/PCA Team Lead responsibilities include, but are not limited to:

- Chair the FCA/PCA,
- Schedule and conduct FCA/PCA kickoff meeting,
- Schedule and prepare FCA/PCA facilities (room, tools, etc.),
- Approve the FCA/PCA plan and implementation instruction,
- Screen action items for accuracy,
- Prepare FCA/PCA Report for submittal,
- Present recommended action item resolutions to SIDS CCMB Chair, and
- Upon closure of all FCA/PCA action items, submit final report to SIDS CCMB Chair and recommend closure of the FCA/PCA.

5.6.3.4. FCA/PCA Team Member

FCA/PCA Team Member responsibilities include, but are not limited to:

- Represent functional area at the FCA/PCA,
- Perform responsibilities as directed by FCA/PCA plan, implementation instruction, and FCA/PCA Team Lead,
- Prepare and use checklists and forms to identify items,
- Prepare and submit to the CM specialist action items to identify anomalies, and
- Prepare and implement proposed resolutions to action items as directed.

5.6.3.5. SIDS Configuration Change Management Board

SIDS CCMB responsibilities include, but are not limited to:

- Recommend FCA/PCA Team members,
- Monitor FCA/PCA progress,
- Recommend approval/disapproval of initial FCA/PCA Reports,
- Review and recommend approval/disapproval of FCA/PCA action item resolutions,
- Report FCA/PCA action items completions to the CCMB Chair, and
- Recommend approval/disapproval of the final FCA/PCA Report.

5.6.3.6. Quality Assurance Representative

The QA Representative(s) responsibilities are:

- Ensure audit team compliance with auditing policies, plans, procedures, and instructions,
- Verify the findings of the audit, and

- Report conflicts or duplications of effort between this section of the CM Plan and Quality Assurance auditing plans and procedures.

5.6.4. FCA/PCA Process

The formal FCA/PCA process begins prior to testing/review. The CM specialist prepares a FCA/PCA Plan for conducting the audit(s). The CM specialist meets with the developer(s) and CI managers to identify relevant system/subsystem team members and prepare detailed instructions for implementing the FCA/PCA. The CM specialist also prepares an agenda, conducts the kickoff meeting, and provides team member instruction where needed. After testing or review is completed, the CM specialist uses a prepared checklist to accumulate all the necessary FCA/PCA materials and documentation for storage in the CML.

5.6.5. SIDS Configuration Management Process Audit

Assigned QA personnel audit CM activities to verify and validate compliance with requirements of VA, OI&T and SIDS CM standards, policies, plans, processes, and procedures. The SIDS CMO Manager will work with the QA Lead to determine auditing schedules, procedures, and instructions. The QA team is requested to audit CM activities in whole or in part at least semi-annually.

5.6.6. SIDS CM Holdings Audit

The CM Manager is responsible for conducting an audit of CM holdings and reporting findings to SIDS CCMB at least annually. The CCMB Chair will appoint at least two non-CMO persons as audit team members. The purpose of the CM Holdings Audit is to verify that all change management artifacts are present and accounted for and that appropriate discrepancy reports are prepared for further action. Prior to the audit, the CMO Manager will indicate to the CCMB whether the entire holdings or portion(s) will be audited. (If the latter, the CCMB Chair will identify the portion(s).) The CMO Manager will prepare a report of audit findings, which the QA team will verify prior to submittal to the CCMB Chair.

5.7. CONTRACTOR/VENDOR CONTROL

The Director, SIDS, has basic responsibility for ensuring:

- Contractor/vendor contractual compliance with the SIDS CM Policy, Plans and Procedures,
- Compliance of contractor/vendor internal CM plans and controls with the provisions of SIDS CM documentation,
- Adequacy of contractor/vendor CM controls for the contracted products and services,
- Adequacy of contractor/vendor CM controls for verification of contractual compliance through test or inspection (or other means as specified by contract), and
- Compatibility of contractor/vendor-supplied equipment, applications, and services with established system configurations is verified.

5.8. REPORTING

The following list of reports will be available from the CM tools or can be generated by a CM specialist with a proficiency in office automation applications such as word processors or spreadsheets.

5.8.1. Action Item List

Any action items that have been generated at a SIDS CCMB meeting are called out in the meeting minutes and are tracked through completion and compiled in the Action Item List. The Action Item List contains, at minimum, the name of the item, description of the action required, team lead and members assigned, latest status, due date, and completion date. SIDS CCMB Chair may require additional information.

5.8.2. CCP Summary History Report

The CCP Summary and History (S&H) Report, issued at least semi-annually, provides a historical summary of all CCPs submitted against all CI within the SIDS organization. Each product/project is responsible for providing the CCP S&H Report to the CCMB membership and the Director, SIDS, or as directed by the Director. The CCP S&H report provides sufficient information for identifying each CCP, its purpose, entities affected, current status, and if applicable, assigned responsibilities. The CM tools will be configured to provide this report. Data included in the CCP S&H report are as follows:

a. CCP number
b. Priority
c. Primary CI affected
d. CCP title/subject
e. Date CCP received by CM group
f. Requested completion date
g. Completion date (if applicable)
h. CCMB date and disposition
i. Current Status
j. Status change date (if other than “Approved”)
k. Incorporation date (blank if not incorporated)
l. Implementation date (blank if not implemented
m. CCMB action date
n. CCMB meeting identifier number
o. CCMB action comments

5.8.3. CCP Status Report

The CCP Status Report, generated monthly, is used to track the status of CCPs from initiation of a CCP through Closure. The CCPs in this report are normally grouped by product as well as status. This report may also be issued as only an Open CCP Status Report or a Closed CCP Status Report. The CCP Status Report contains at least the following information:

a. CCP number
b. Priority
c. Primary CI affected
d. CP title/subject
e. Originator group
f. Date CCP received by CM group
g. Requested completion date
h. ECCMB action date and disposition
i. Current status
j. Status change date
k. Current action team
l. Impacted organizations
p. Remarks

5.8.4. Closed CCP Report

The Closed CCP Report (issued upon request) provides the same information as the CCP Status Report; however, the report includes only CCPs that have been assigned a status of "Closed." The Closed CCP Report is normally used for CCM performance metrics.

5.8.5. CM Internal Audit Report

The CMO Manager prepares the CM Internal Audit Report for SIDS CCMB after conducting an examination of CM holdings. The report contains the date(s) of the audit and accompanying audit team members, identifies the portion(s) of holdings audited, and enumerates missing items or discrepancies found.

5.8.6. CM Process Audit Report

The QA person who conducted the CM process audit prepares the CM Process Audit Report to inform the Director, SIDS, SIDS CCMB Chair and CCMB membership, and the CM Manager of organizational compliance with CM policies, plans, processes and procedures. The QA group is responsible for the form, format, and content of the report.

5.8.7. COTS Software Baselines Report

The COTS Software Baselines report contains a listing of all approved COTS packages available for use on the network over which SIDS has responsibility and authority. A COTS "package" includes, but is not limited to: the COTS item as delivered, all patches, all builds, and all upgrades. The CM group provides the COTS Software Baseline Report upon request.

5.8.8. Functional Configuration Audit Report

The assigned audit team lead prepares a Functional Configuration Audit (FCA) Report after each FCA to inform SIDS CCMB Chair and other senior management of discrepancies (if any) between functional attributes and requirements specified in product definition information and those achieved. The FCA Report contains such information as (but not limited to):

a. Date(s) of the audit,
b. Audit team lead,
c. Audit team members,
d. Portion(s) of the product or system/sub-system audited,
e. Identity of the functional requirements documentation used,
f. Identity of the audit criteria documentation used, and
g. Enumerated listing of failures (specific requirement, specific criteria failed, degree of failure (if applicable), and comments).

5.8.9. Closed CCP Report

The Closed CCP Report (issued upon request) provides the same information as the CCP Status Report; however, the report includes only CCPs that have been assigned a status of "Closed," i.e., those that have been fully implemented, disapproved, or withdrawn. The Closed CCP Report is normally used for CCM performance metrics.

5.8.10. Physical Configuration Audit Report

The assigned audit team lead prepares a Physical Configuration Audit (PCA) Report after each PCA to inform SIDS CCMB and other senior management of discrepancies (1) between product design and product definition information, and (2) between product operational information and product definition information. The PCA Report contains such information as (but not limited to):

a. Date(s) of the audit,
b. Audit team lead and audit team members,
c. Portion(s) of the product or system/sub-system audited,
d. Identity of the baselines used,
e. Identity of the audit criteria documentation used, and
f. Enumerated listing of failures (specific design element, specific production definition line item, description of the discrepancy, and comments).

5.8.11. Product Status Report

The Product Status Report contains the same information as the Open CCP Status Report but includes "Closed" CCPs. Provided upon request of the product owner, this report allows the reader to focus on CCPs against an individual product or component; therefore, the data is sorted and reported according to the product. The Product Status Report contains the following information:

a. Primary CI affected
b. CCP number
c. Priority
d. CP title/subject
e. Originator group
f. Date CCP received by CM group
g. Requested completion date

h. ECCMB action date and disposition
i. Current status
j. Status change date
k. Current action team
l. Impacted organizations
m. Remarks

5.8.12. Product Version Description

The Product Version Description (PVD) is developed for each deliverable product, and is a component of the deliverable package. A PVD lists all components of the product comprising its current version, methods used to install the entity, and methods and tools used to test the system. Minimum information for each component includes but is not limited to:

a. Identification numbers,
b. Names or titles,
c. Component Version/Release Numbers,
d. General type of component (e.g. Document, Source Code, Executable, Access Database, etc.),
e. Dates of Issue, and
f. Form of Media (e.g. Hard Copy, Tape, Diskette, etc.).

5.8.13. SIDS CCMB Meeting Minutes

The SIDS CCMB Secretariat shall prepare and distribute CCMB Meeting Minutes to report pertinent comments, actions, and decisions that occurred during each CCMB meeting. The CCMB shall determine a standard minutes distribution list to include, but not limited to:

- Director, SIDS,
- VA Deputy CIO,
- ADAS EAM,
- Director of each EAM Service,
- Head of each SIDS Staff Element,
- CCMB Chair,
- All voting and advisory members of the CCMB,
- CCMB Secretariat, and
- CMO Manager.

The draft shall be submitted to the CCMB membership for review no later than 10 working days after the meeting (unless the CCMB authorizes an extension). The membership offers corrections at the next meeting. As soon as the corrections are incorporated and verified (but not more than 5 working days following the close of the meeting), the minutes are disseminated to the distribution list.

APPENDIX A – TERMS AND ABBREVIATIONS

A.1. TERMS AND DEFINITIONS

These terms are used in this plan in the context of CM. The adjoining definitions are taken from the references, as indicated, in Section 2 of the main body. (Refer to page 4.)

TERM	DEFINITION
allocated requirement	requirement that levies all or part of the performance and functionality of a higher level requirement on a lower level architectural element or design component (CMU/SEI CMMI)
approval	authorization from a designated authority that a product, process, or information is complete and suitable for use (GEIA-649)
archived information	information that has been retained for historical purposes and that can be retrieved and is usable over the time designated for retention (GEIA-649)
attributes	refer to "product attributes" (GEIA-649)
audit	independent examination of a work product or set of work products to determine whether requirements are being met (CMU/SEI CMMI)
baseline	refer to "configuration baseline" (GEIA-649)
change	refer to "configuration change" (GEIA-649)
change approval authority	activity (usually represented by a person or defined group of persons) authorized to approve any configuration change to a product **and** to commit resources for its implementation. (GEIA-649)
change management	judicious use of means to effect a change, or proposed change, on a product or service. (Refer to "configuration management.") (CMU/SEI CMMI)
concept of operations	general description of the way in which an entity is used or operates (CMU/SEI CMMI)
configuration	(1) product attributes of an existing or planned product or combination of products; (2) one of a series of sequentially-created variations of a product (GEIA-649)
configuration audit	CM function that reviews processes and products to validate compliance with requirement, and verifies that products have achieved their required attributes and conform to released product definition information. Configuration audits may be divided into separate functional and physical configuration audits (GEIA-649)

TERM	DEFINITION
configuration baseline	1. agreed-to information that identifies and establishes the attributes of a product at a point in time **and** that serves as basis for defining change (GEIA-649) 2. The configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. (CMU/SEI CMMI)
configuration change	an alteration to a product and/or its product configuration information (as documented in a request for change) (GEIA-649)
configuration change management	CM function that ensures changes to a configuration baseline are properly identified, recorded, evaluated, approved or disapproved, and incorporated and verified as appropriate (GEIA-649)
configuration change management board	group of persons responsible for evaluating and forming a recommendation for proposed changes (for approval or disapproval) to configuration items, and for ensuring implementation of approved changes. (CMU/SEI CMMI) Also known as “change control board.” or “configuration control board”
configuration identification	CM function that: a. establishes a structure for products and product configuration information; b. selects, defines, documents, and baselines product attributes; and c. assigns unique identifiers to each product and product configuration information (GEIA-649)
configuration item	work product or aggregation of work products designated for configuration change management and treated as a single entity in the configuration management process (CMU/SEI CMMI)
configuration management	process that establishes and maintains consistency of a product’s attributes with its requirements and product configuration information throughout the product’s life cycle (GEIA-649)

TERM	DEFINITION
configuration status accounting	(1) CM function managing the capture and maintenance of product configuration information necessary to account for the configuration of a product throughout the product's life cycle (GEIA-649) (2) element of CM consisting of the recording and reporting of information needed to manage a configuration effectively. (This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes (CMU/SEI CMMI)
configuration verification	CM function that ascertains that a product has achieved consistency and accuracy of its product requirements and product configuration information (GEIA-649)
customer	party (individual, project, or organization) responsible for accepting the product or for authorizing payment. The customer is external to the project, but not necessarily external to the organization (CMU/SEI CMMI)
design information	technical information resulting from translating requirements for a product into a complete description of the product. Refer to "product definition information.) (GEIA-649)
disapproval	conclusion by the appropriate authority that a product, a process, or information is incomplete or unsuitable for its intended use.
document	self-contained body of information or data that can be packaged for delivery on a single medium. Examples include: drawings, reports, standards, databases, application software, engineering designs, virtual-part model. NOTE: medium may be paper, photograph, digital files, optical, magnetic, electronic storage, or a combination. (GEIA-649)
enterprise	the larger organizational entity not always reached by the word "organization." An enterprise may consist of many organizations in many different locations with different customers. The word "enterprise" refers to the full composition of organizations. (CMU/SEI CMMI)
form	shape, size, Dimensions™, and other physically measurable parameters that characterize a product (GEIA-649)
function	action or actions that a product is designed to perform

TERM	DEFINITION
functional attributes	measurable performance parameters expressed in quantitative terms; e.g., range, speed, reliability, maintainability, safety, and operating and logistical parameters (including tolerances) (GEIA-649)
hardware	products and their components; e.g., mechanical, electrical, electronic, hydraulic, pneumatic, made of material (GEIA-649)
information technology architecture	integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals (Clinger-Cohen Act, 1996)
interface control	process of identifying, recording, and managing product attributes at the common boundary of two or more products provided by one or more organizations (GEIA-649)
interface	product attributes that exist at a common boundary of two or more products (GEIA-649) (or product components)
life cycle	generic term for the phases in the life of a product from concept to disposal (GEIA-649)
metadata	information about data (GEIA-649)
operational environment	set of conditions in which the product(s) is designed to be used (GEIA-649)
performance	quantitative measure characterizing a physical or functional attribute relating to the execution of an operation or function (e.g., quantity (how many/how much), quality (how well), coverage (how much area, how far), timeliness (how responsive, how frequent), and readiness (availability, mission/operational readiness) (GEIA-649)
product	(1) something used or produced to satisfy a need or is the result of a process; e.g., document, facility, firmware, hardware, materials, processes, services, software, systems (GEIA-649) (2) any tangible output or service that is a result of a process and that is intended for delivery to a customer or end user. A product is a work product that is delivered to the customer. (CMU/SEI CMMI)
product attributes	performance, functional, and physical characteristic(s) of a product (GEIA-649)
product configuration information	information about a product consisting of product definition information and product operational information (GEIA-649)

TERM	DEFINITION
product definition information	information that defines the product requirements, documents the product attributes, and is the authoritative source for configuration definition and control (GEIA-649)
product identifier	name or alphanumeric identifier, unique to the issuing organization, used to designate products of the same configuration, and to differentiate them from other products (GEIA-649)
product operational information	information developed from product definition information and used to test, operate, maintain, and dispose of the product (GEIA-649)
product requirements	refinement of customer requirements into developers' language, making implicit requirements into explicit derived requirements. (The developer uses the product requirements to guide the design and building of the product.) (CMU/SEI CMMI)
product structure	a hierarchical view of the relationship of products and components products (GEIA-649)
quality assurance	planned and systematic means for assuring management that defined standards, practices, procedures, and methods of the process are applied (CMU/SEI CMMI)
quality control	operational techniques and activities that are used to fulfill requirements for quality. (CMU/SEI CMMI [ISO 8402-1994])
release	(1) particular version or revision of a product that is made available for a specific purpose (for example, test release, production release) (GEIA-649); (2) authorization for dissemination of approved information and/or products subject to configuration change management (GEIA-649); (3) a baseline that serves as the basis for further work outside the function that created it (for example, requirements baseline released for design work)
requirement	(1) need or expectation that is stated and obligatory; (2) specified value for an essential product attribute (GEIA-649)
requirements traceability	evidence of an association between a requirement and its source requirement, its implementation, and its verification (CMU/SEI CMMI)
retrofit	as the result of an approved configuration change, the incorporation of new design part(s), or software code, into products already delivered (GEIA-649)

TERM	DEFINITION
revision	result of updating a product or product configuration information (Refer to also version) (GEIA-649) NOTE: Revision numbers are incremented each time the product or product configuration information is modified, regardless of version or release action
specification	information that explicitly states the requirements for product attributes (GEIA-649)
technical environment	set of conditions in which the product(s) is designed to be built (GEIA-649)
validation	(1) authentication that the requirements for specific intended use or application have been fulfilled (GEIA-649) (2) confirmation that the product, as provided, will fulfill its intended use. Validation ensures that "you built the right thing." (CMU/SEI CMMI)
variance	approved departure from a specified requirement(s) that does not require revision of approved product definition information (GEIA-649)
verification	(1) confirmation that a specified requirement has been fulfilled by the product(GEIA-649) (2) confirmation that work products properly reflect the requirements specified for them. Verification ensures that "you built it right." (CMU/SEI CMMI)
version	specific configuration of a product which varies from other configurations of the product (GEIA-649)

A.2. ABBREVIATIONS AND ACRONYMS

The following abbreviations and acronyms are used in this plan.

ABBREVIATION	EXPANSION
CCM	Configuration Change Management
CCMB	Configuration Change Management Board
CCP	Configuration Change Proposal
CDR	Critical Design Review
CI	Configuration Item
CIO	Chief Information Officer
CM	Configuration Management
CML	Configuration Management Library
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMU	Carnegie-Mellon University
CONOP	Concept of Operations
COTS	Commercial-Off-The-Shelf (usually software)
CSA	Configuration Status Accounting
DR	Discrepancy Report
EA	Enterprise Architecture
EIA	Electronic Industries Alliance
EIB	Enterprise Information Board
FCA	Functional Configuration Audit
FRR	Functional Readiness Review
GEIA	Government Electronics and Information Technology Association
GOTS	Government-modified COTS
IDE	Integrated Development Environment
IRR	Initiation Readiness Review
IT	Information Technology
MOTS	Modified COTS (usually software)
NCR	Non-Compliance Report
OI&T	Office of Information and Technology
ORR	Operations Readiness Review
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PR	Problem Report
PVD	Product Version Description

ABBREVIATION	EXPANSION
QA	Quality Assurance
RFW	Request for Waiver
RTM	Requirements Traceability Matrix
S&H	Summary and History
SDLC	Systems Development Life Cycle
SEI	Software Engineering Institute
SIDS	Systems Integration and Development Services
SME	Subject Matter Expert
SRS	System/Subsystem Requirements Specification
SSS	System/Subsystem Specification
TIR	Test Incident Report
TPR	Test Problem Report
TRR	Test Readiness Review
TT	Trouble Ticket
VA	(Department of) Veterans Affairs

APPENDIX B – BASELINE REVIEWS

The following paragraphs describe some of the reviews and formal baselines that the VA OI&T may require. Excepting the Business Case Review, baselines to be presented for these reviews are established prior to the review (i.e., resulting changes and modifications will be submitted against these "snapshots-in-time").

B.1. BUSINESS CASE REVIEW

The Business Case Review is conducted by enterprise architecture, budget, and technical authorities prior to commencement and outside of project work to determine if the proposed product or service appears to be worthwhile, cost effective, and technically feasible and to authorize the time and expense necessary to develop it. Typical initiation stage artifacts may include a statement of need, a description of the finished product or service, some form of cost-benefit report, and an approval document or memo. These artifacts may be turned over to the CM office (for requirements traceability purposes) upon approval of the project or may be kept in management files due to possible financial or other sensitivities.

B.2. INITIATION READINESS REVIEW

An Initiation Readiness Review (IRR) is conducted by organizational management authorities, technical authorities, and the proposed project team organization to analyze the product, the Concept(s) of Operations (CONOP), and project management structure and scheme (1) to ensure that the conceptual design satisfies the stated need, (2) that it is operationally sound, and (3) that the proposed project team organization is appropriate and adequate for the project.

Some typical items for this review include the CONOP and drafts of high-level functional requirements, infrastructure planning, initial project plan, and appropriate life cycle tailoring. (In some instances, the CONOP may be required for the Business Case Review.) Other items may be included such as initial plans for Acquisition, Configuration Management, Quality Assurance, and System Security. Baseline changes resulting from the review are documented and incorporated (through formal change management processes if possible) and resubmitted to the IRR.

B.3. FUNCTIONAL REQUIREMENTS REVIEW

During the Functional Requirements Review (FRR), the "customer(s)" and the project management team conduct the Functional Requirements Review (FRR) to ensure a complete and accurate understanding of what the product is to provide or accomplish and that the project management pieces are in place to produce it. Functional requirements and project management documentation must be placed under formal CCM prior to the FRR to provide bi-directional traceability with the CONOP and for changes that may result from the review and to eliminate the danger of unauthorized pen-and-ink changes. (Documentation with a complex set of functional requirements will probably be placed under formal configuration control at an early point in the drafting.) The FRR may be revisited until there is an agreed-upon set of functional requirements.

Typical items provided from the CML may include the functional requirements baseline (also known as the Functional Requirements Document or System/Subsystem Specification (SSS), the Test and Evaluation Master Plan, the Interface Control Document, and an initial Requirements Traceability Matrix (RTM).

B.4. DESIGN REVIEW

Design reviews are conducted to ensure that functional requirements have been properly and correctly allocated to appropriate system/product resources and then transformed into complete, defined, and detailed specifications for the system/product components. The decisions made in this phase address in detail how the system/product will meet the defined functional, physical, interface, and data requirements. Results of design reviews guide the work during development.

Depending upon the complexity of the product, design reviews may be divided into a Preliminary Design Review (PDR) for the general system/product design and a Critical Design Review (CDR) for the detailed system/product design. A PDR is conducted to evaluate the design approach and technical adequacy, to determine design compatibility with requirements, and, as applicable, to evaluate preliminary operational and support documents for the product.

During a CDR, the review team reviews preliminary product specifications:

(1) To ensure that the system/product specifications satisfy functional capability requirements,
(2) To evaluate preliminary test planning,
(3) To evaluate the adequacy of preliminary operation and support documentation,
(4) To ensure that configuration items and other items of equipment, facilities, software, and personnel are compatible, and
(5) To ensure that risk areas have been adequately addressed.

Design phase activities may be conducted in an iterative fashion between PDR and CDR as it evolves through the design phase. The following is a sample list of items provided by the CML for the design review(s):

Technical: Functional requirements document (System-Subsystem Specification, (SSS)), detailed requirements specification document (System/Subsystem Requirements Specification (SRS)), Requirements Traceability Matrix (RTM), application functional design(s), application physical design(s), specification lists, implementation plan, maintenance manual, operations manual, training plan and materials, conversion, migration/transition strategy designs, facilities drawings, wiring diagrams, connection schematics, etc.

Management: Final Configuration Management (CM) Plan, Final Quality Assurance (QA) Plan, System Test Plan, Data Management Plan, Implementation Plan, Deployment Plan, Project Risk Management Plan and Project Risks Database, Security Plan, Security Risk Assessment, Draft Security Test Plan, Interconnection Security Agreements.

B.5. TEST READINESS REVIEWS

Proper Test Readiness Reviews (TRR) ensure that a product or component is prepared to proceed to formal testing by verifying that test plans, test procedures, facilities, personnel and other required resources are (1) available, (2) complete, (3) comply with test plans and descriptions, and (4) satisfy testing requirements. A TRR may be required for unit tests, system tests, integration tests, regression tests, and acceptance tests. The TRR for each type of test may have a different team of reviewers.

For a TRR, the CML provides (depending upon the test to be conducted) such baselines as: requirements traceability matrix (RTM), test plan (system test plan, security test plan, acceptance test plan), test cases/scenarios, source code, source code documentation (e.g., flowcharts, comments), executable code, databases, data management plan, infrastructure documentation, training plan, training materials, design documents, user's guide, operations manual, project plan, risk management plan, risk mitigation plans, contingency plan, disaster recovery plan, etc.

B.6. OPERATIONS READINESS REVIEW

An Operations Readiness Review (ORR) is used to ensure that the product package being delivered has been properly tested and is complete, correct, and correctly identified in all respects.

Items from the CML for the ORR include: system acceptance test results, problem reports, system acceptance sign-off document, user acceptance test results, problem reports, user acceptance sign-off memo, approved user documentation and training materials, security certification package, security accreditation package, security plan, security risk assessment, security features user's guide, production-ready code, production-ready facilities documentation, blueprints, schematics, and diagrams, final documents, implementation and deployment plans, operations manuals, system and documentation baselines, move-initiation requests, version descriptions, etc.

B.7. OTHER REVIEWS

Other reviews may be called out by the CCMB or Project Manager who will work with the CM librarian to define the baseline components to be provided for each specific review.

APPENDIX C – CHANGE DOCUMENT RELATIONSHIPS

C.1. NON-CONFORMANCE REPORTING

Non-Conformance Reporting is a change control method used to report incongruities revealed during reviews, tests, and audits of a CI prior to establishment of the production baseline. The non-conformance reporting family includes the Discrepancy Report (DR), the Test Incident Report (TIR, also called a Problem Report), and the Non-Compliance Report (NCR).

The DR and the TIR are used as interfaces between the tester, reviewer, or Quality Assurance official and the CI manager. The TIR designation is reserved for product test/review results; all other product defects are reported via the DR. The NCR is used as the interface between a Quality Assurance official and management personnel to report non-compliance with policies, plans, processes, and procedures.

Upon submittal, a non-conformance report is forwarded to the responsible product manager. The product manager reviews the report to determine if the issue requires a CCP for resolution.

The CM group will use the CM tool to track non-conformance reports from initiation through closure.

NOTE: A DR/TIR/NCR may spawn a CCP. A CCP shall never spawn a DR, TIR, or NCR.

C.2. HELP-LINE TICKET REPORTING

Users often report difficulties with a deployed operational baseline to the Help Desk, which in turn generates Help-line Tickets (also called Trouble Ticket) to report user problems. If a Help Desk technician determines that a solution requires a change or modification to a CI, the Help Desk prepares an appropriate CCP and submits it to initiate CCP processing. As the originating organization of the CCP, the Help Desk shall be notified when the proposed CCP solution has been implemented operationally.

The Help Desk tracks Help-line Tickets.

NOTE: A Help-line Ticket may spawn a CCP. A CCP shall never spawn a Help-line Ticket.